Referenzhandbuch für den RangeMax Wireless Router WPN824

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10097-01
Mai 2005

© 2005 by NETGEAR, Inc. Alle Rechte vorbehalten. Mai 2005.

Marken

NETGEAR ist eine Marke von NETGEAR, Inc.

Microsoft, Windows und Windows NT sind eingetragene Marken der Microsoft Corporation.

Andere Marken- und Produktnamen sind eingetragene Marken oder Marken der jeweiligen Inhaber.

Nutzungsbedingungen

Zur Verbesserung des internen Designs, des Betriebs und/oder der Zuverlässigkeit behält NETGEAR sich das Recht vor, die in diesem Dokument beschriebenen Produkte ohne vorherige Ankündigung zu ändern.

NETGEAR lehnt im Zusammenhang mit dem Einsatz oder der Anwendung der hier beschriebenen Produkte oder Schaltpläne jegliche Haftung ab.

Federal Communications Commission (FCC) – Hochfrequenzhinweise

Dieses Gerät wurde geprüft, und es wurde festgestellt, dass es die Grenzwerte für Digitalgeräte der Klasse B gemäß Teil 15 der FCC-Vorschriften einhält. Diese Grenzwerte sind für die Gewährleistung eines angemessenen Schutzes gegen schädliche Störungen bei Installation im Wohnbereich gedacht. Dieses Gerät erzeugt und benutzt hochfrequente Energien und kann diese abstrahlen. Wenn es nicht in Übereinstimmung mit den Anleitungen installiert und verwendet wird, kann es den Rundfunkempfang erheblich beeinträchtigen. Bei keiner Installation können Störungen jedoch völlig ausgeschlossen werden. Wenn dieses Gerät Störungen des Rundfunk- und Fernsehempfangs verursacht, was durch Ein- und Ausschalten des Gerätes festgestellt werden kann, sollte der Benutzer versuchen, die Störung durch eine oder mehrere der folgenden Maßnahmen zu beheben:

- Platzieren Sie die Empfangsantenne an einer anderen Stelle bzw. richten Sie sie neu aus.
- Vergrößern Sie den Abstand zwischen dem Gerät und dem Empfänger.
- Schließen Sie das Gerät an einen Stromkreis an, den der Empfänger nicht benutzt.
- Wenden Sie sich an den Händler oder einen erfahrenen Rundfunk-/TV-Techniker.

EN 55 022 – Erklärung zur Konformität

Hiermit wird bestätigt, dass der RangeMax Wireless Router WPN824 gemäß der EU-Richtlinie 89/336/EWG, Artikel 4a, gegen die Erzeugung von Funkstörungen abgeschirmt ist. Die Konformität wird durch Anwendung von EN 55 022 Klasse B (CISPR 22) bestätigt.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, dass der RangeMax Wireless Router WPN824 gemäß den im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z. B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, dass dieses Gerät auf den Markt gebracht wurde, und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, dass der RangeMax Wireless Router WPN824 gemäß den im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z. B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, dass dieses Gerät auf den Markt gebracht wurde, und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

VCCI (Voluntary Control Council for Interference) – Erklärung

Dieses Gerät gehört der Kategorie 2 (Informationsgeräte für den Einsatz in Wohngebieten und angrenzenden Gebieten) an und erfüllt die Standards des Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines zur Verhinderung von Funkstörungen in Wohngebieten.

Wenn dieses Gerät in der Nähe eines Radios oder Fernsehgeräts aufgestellt wird, kann es Funkstörungen verursachen.

Lesen Sie bitte die Hinweise zur korrekten Handhabung.

Kundensupport

Beachten Sie die Karte mit den Support-Informationen, die dem RangeMax Wireless Router WPN824 beigefügt ist.

Internet

Die Website von NETGEAR finden Sie unter der folgenden URL:
http://www.netgear.de. Dazu sind eine direkte Internetverbindung und ein Webbrowser (z. B. Internet Explorer oder Netscape) erforderlich.

Produkt- und Dokumentationsinformationen

Modellnummer:	WPN824
Erscheinungsdatum:	Mai 2005
Produktfamilie:	Router
Produktname:	RangeMax Wireless Router WPN824
Produkt für privaten oder kommerziellen Gebrauch:	Heim
Sprache:	Deutsch
Artikelnummer des Dokuments:	202-10097-01

Inhalt

Kapitel 1
Informationen zu diesem Handbuch

Zielgruppe, Gültigkeit, Konventionen und Formate 1-1
Zur Verwendung dieses Handbuchs 1-2
Ausdrucken dieses Handbuchs 1-3

Kapitel 2
Einführung

Die wichtigsten Merkmale 2-1
MIMO-basierte RangeMax™-Technik (Multi-In, Multi-Out) 2-2
Drahtlose 802.11g-Netzwerke 2-2
Leistungsstarke, echte Firewall mit Content-Filterung 2-3
Sicherheit 2-3
Netzwerkverbindungen mit automatischer Erkennung durch Auto Uplink 2-4
Umfassende Unterstützung gängiger Protokolle 2-4
Einfache Installation und Verwaltung 2-5
Wartung und Support 2-5
Verwandte NETGEAR-Produkte 2-6
Lieferumfang 2-6
Vorderseite des Routers 2-6
Rückseite des Routers 2-7
Eine Übersicht für den „Weg zum Erfolg“ 2-8

Kapitel 3
Verbindung des Routers mit dem Internet

Vorbereitung der Installation Ihres Wireless Routers 3-1
Konfigurieren Sie den Wireless Router zunächst mit dem Smart Wizard 3-2
Richten Sie jetzt einen Computer für drahtlose Verbindungen ein 3-3
Tipps zur Fehlerbehebung 3-4
Überblick über die Zugriffsmöglichkeiten auf den Wireless Router 3-5

So melden Sie sich nach dem Übernehmen der Konfigurationseinstellungen beim Wireless Router an 3-6
So umgehen Sie den Konfigurationsassistenten 3-8
So konfigurieren Sie Ihre Internetverbindung manuell 3-9
Verwendung des Setup-Assistenten 3-12
NETGEAR Produktregistrierung, Support und Dokumentation 3-12

Kapitel 4
WLAN-Konfiguration

Hinweise zur Leistung, Aufstellung und Reichweite 4-1
Angemessene Sicherheitsmaßnahmen für Ihr drahtloses Netzwerk 4-2
Erläuterung der WLAN-Einstellungen 4-4
Erforderliche Information vor der Änderung grundlegender WLAN-Einstellungen 4-7
Werkseitige Voreinstellungen 4-8
So richten Sie eine erste drahtlose Verbindung ein und testen sie 4-8
So konfigurieren Sie WEP 4-10
So konfigurieren Sie WPA-PSK-Sicherheit im drahtlosen Netzwerk 4-12
So schränken Sie den Zugang auf drahtlose Netzwerke über die MAC-Adresse ein 4-13

Kapitel 5
Content-Filterung

Überblick über die Content-Filterung 5-1
Sperren des Zugriffs auf Internet-Websites 5-2
Sperren des Zugriffs auf Internetdienste 5-3
Einrichten eines benutzerdefinierten Dienstes 5-4
Sperren von Diensten für bestimmte IP-Adressen 5-5
Sperrungen zu bestimmten Zeiten 5-5
Ansehen von Protokollen für Internetzugriff oder versuchten Zugriff 5-6
Einrichten von Benachrichtigungen und Zugriffswarnungen per E-Mail 5-7

Kapitel 6
Wartung

Anzeigen der Statusinformationen des Wireless Routers 6-1
Anzeigen der angeschlossenen Geräte 6-5
Verwaltung der Konfigurationsdateien 6-6
Wiederherstellung und Sichern der Konfiguration 6-6
Löschen der Konfiguration 6-7
Aktualisieren der Routersoftware 6-7
Ändern des Administratorpassworts 6-9

Kapitel 7
Fehlerbehebung

Basisbetrieb 7-1
Stromanzeige leuchtet nicht 7-1
Anzeigen erlöschen nicht 7-2
Die LAN- oder WAN-Portanzeige leuchtet nicht 7-2
Netzwerkkonfigurationsoberfläche 7-3
Internetverbindung 7-4
TCP/IP-Netzwerke mit einem Ping-Dienstprogramm prüfen 7-5
Testen des LAN-Pfads zum Router 7-5
Testen des Pfads vom Computer zu einem entfernten Gerät 7-6
Wiederherstellen von Werkseinstellungen und Passwort 7-7
Probleme mit Datum und Uhrzeit 7-8

Kapitel 8
Erweiterte Routerkonfiguration

Konfiguration der erweiterten WLAN-Einstellungen 8-1
Liste der zugriffsberechtigten WLAN-Karten 8-3
WLAN-Karten einrichten 8-4
Konfiguration von Port-Triggering und Portweiterleitung 8-5
Konfiguration der Portweiterleitung an lokale Server 8-8
Hinzufügen eines benutzerdefinierten Dienstes 8-9
Bearbeiten oder Löschen eines Portweiterleitungseintrags 8-10
Beispiel: Lokaler Web- und FTP-Server 8-10
Beispiel: Half Life, KALI oder Quake III mit mehreren Computern 8-10
WAN-Konfigurationsoptionen 8-11
Bei Bedarf automatisch verbinden 8-11
Deaktivieren der SPI-Firewall 8-12
Einrichten eines Exposed Host (DMZ) 8-12
Ermöglichen von Reaktionen auf Ping-Anforderungen am Internet-WAN-Port 8-12
Einstellen der MTU-Größe 8-13
Verwendung der LAN-IP-Konfigurationsoptionen 8-13
LAN-TCP/IP-Parameter 8-14
Einsatz des Routers als DHCP-Server 8-15
Reservieren von Adressen 8-16
Verwendung von dynamischen DNS-Diensten (DDNS) 8-16

Konfiguration statischer Routen 8-17
Ermöglichen der Fernsteuerung 8-19
Verwendung von Universal Plug and Play (UPnP) 8-20

Anhang A
Technische Daten

Anhang B
Netzwerke, Routing, Firewalls und Grundlagen

Weiterführende Dokumente B-1
Grundlegende Routerkonzepte B-1
Was ist ein Router? B-1
RIP (Routing Information Protocol) B-2
IP-Adressen und das Internet B-2
Netzmaske B-4
Subnetzadressierung B-4
Private IP-Adressen B-7
Betrieb mit einer einzelnen IP-Adresse mit Hilfe von NAT B-7
MAC-Adressen und ARP (Address Resolution Protocol) B-8
Weiterführende Dokumente B-9
DNS-Server B-9
IP-Konfiguration über DHCP B-10
Internetsicherheit und Firewalls B-10
Was ist eine Firewall? B-10
SPI (Stateful Packet Inspection) B-11
Denial-of-Service-Angriffe B-11
Netzwerk-Verkabelung B-11
Kabel der Kategorie 5 ..... B-12
Das Innenleben eines Twisted-Pair-Kabels B-13
Uplink-Switches, Crossover-Kabel und MDI-/MDIX-Umschaltung B-14

Anhang C
Netzwerkeinrichtung

Voraussetzungen zum Einsatz eines Routers mit einem Breitbandmodem C-1
Kabel und Computer-Hardware C-1
Netzwerkkonfiguration des Computers C-1
Konfiguration des Internetzugangs C-2
Wo erhalte ich die Parameter für die Internetkonfiguration? C-2

Aufzeichnung der Internetzugangsdaten C-3
Einrichten der Computer für den TCP/IP-Netzwerkbetrieb C-4
Einrichten von Windows 95, 98 und Me für den TCP/IP-Netzwerkbetrieb C-5
Installieren oder Überprüfen der Windows-Netzwerkkomponenten C-5
Einrichten von DHCP zur automatischen Konfiguration von TCP/IP-Einstellungen unter Windows 95B, 98 und Me C-6
Auswählen der Internetzugriffsmethode unter Windows C-8
Überprüfen der TCP/IP-Eigenschaften C-8
Einrichten von Windows NT4, 2000 oder XP für den IP-Netzwerkbetrieb C-9
Installieren oder Überprüfen der Windows-Netzwerkkomponenten C-9
DHCP-Konfiguration von TCP/IP unter Windows XP, 2000 oder NT4 ..... C-10
DHCP-Konfiguration von TCP/IP unter Windows XP C-10
DHCP-Konfiguration von TCP/IP unter Windows 2000 ..... C-12
DHCP-Konfiguration von TCP/IP unter Windows NT4 ..... C-15
Überprüfen der TCP/IP-Eigenschaften unter Windows XP, 2000 und NT4 ..... C-17
Einrichten eines Apple-Computers für den TCP/IP-Netzwerkbetrieb C-18
Mac OS 8.6 oder 9.x C-18
Mac OS X C-18
Überprüfen der TCP/IP-Eigenschaften bei Apple-Computern C-19
Überprüfen der Bereitschaft des Internetzugangs C-20
Werden Anmeldeprotokolle verwendet? C-20
Wie lauten Ihre Konfigurationsdaten? C-20
Ermitteln der ISP-Konfigurationsdaten für Windows-Computer C-21
Ermitteln der ISP-Konfigurationsdaten für Apple-Computer C-22
Neustarten des Netzwerks C-23

Anhang D
Grundlagen drahtloser Netzwerke

Überblick über drahtlose Netzwerke D-1
Infrastruktur-Modus D-1
Ad-hoc-Modus (Peer-to-Peer-Arbeitsgruppe) D-2
Netzwerkname: ESSID (Extended Service Set Identifier) D-2
Authentifizierung und WEP-Datenverschlüsselung D-2
802.11-Authentifizierung D-3
Open-System-Authentifizierung D-3
Shared-Key-Authentifizierung D-4

Überblick über die WEP-Parameter D-5
Schlüsseltiefe D-6
WEP-Konfigurationsoptionen D-7
Drahtlose Kanäle D-7
Sicherheit im drahtlosen Netzwerk mit WPA und WPA2 ..... D-8
Worin unterscheidet sich WPA von WEP? D-9
Worin unterscheidet sich WPA von WPA 2 (IEEE 802.11i)? D-10
Was sind die Hauptsicherheitsmerkmale von WPA und WPA2? D-10
WPA-/WPA2-Authentifizierung: Benutzerauthentifizierung in Unternehmensnetzwerken über 802.1x/EAP und RADIUS D-12
WPA-/WPA2-Schlüsselverwaltung D-14
Sind mit WPA/WPA2 alle Probleme gelöst? D-16
Produktunterstützung für WPA/WPA2 ..... D-16
Änderungen an Wireless Access Points D-17
Änderungen an drahtlosen Netzwerkadaptern D-17
Änderungen an Programmen für drahtlose Clients D-18
Glossar

Kapitel 1
Informationen zu diesem Handbuch

In diesem Kapitel werden die angesprochene Zielgruppe sowie Gültigkeit, Konventionen und Formate dieses Handbuchs beschrieben.

Zielgruppe, Gültigkeit, Konventionen und Formate

Das vorliegende Referenzhandbuch wendet sich an Leser, die über grundlegende bis fortgeschrittene Computer- und Internetkenntnisse verfügen. In den Anhängen und auf der NETGEAR-Website finden Sie jedoch die Grundlagen zu Computernetzwerken, Internet, Firewall- und VPN-Technik.

Im vorliegenden Handbuch gelten die folgenden Schriftkonventionen:

Tabelle 1-1. Schriftkonventionen

Kursivdruck	Betonung, Buchtitel, CDs, URLs
Fettdruck	Benutzereingaben, Optionen
`Courier`	Bildschirmtext, Datei- und Servernamen, Dateierweiterungen, Befehle, IP-Adressen

Im vorliegenden Handbuch werden die folgenden Formate zur Hervorhebung besonderer Hinweise verwendet:

Hinweis: Mit diesem Format werden Informationen von besonderer Bedeutung oder besonderem Interesse hervorgehoben.

Dieses Handbuch wurde entsprechend den folgenden Vorgaben für den WPN824 Router verfasst:

Tabelle 1-2. Gültigkeit des Handbuchs

Produktversion	RangeMax Wireless Router WPN824
Datum der Veröffentlichung	Mai 2005

Zur Verwendung dieses Handbuchs

Die HTML-Version dieses Handbuchs enthält folgende Zusatzfunktionen:

- Die Schaltflächen > und < zum Vor- und Zurückblättern durch das Handbuch.
- Die Schaltfläche Inhalt zum Aufrufen des Inhaltsverzeichnisses und die Schaltfläche Index. Doppelklicken Sie auf einen Link im Inhaltsverzeichnis oder Index, um direkt an die Stelle im Handbuch zu gelangen, an der dieses Thema behandelt wird.
- Die Schaltfläche Online-Wissensdatenbank für den Zugriff auf die komplette NETGEAR, Inc. Online-Wissensdatenbank für das Produktmodell.
- Links zu PDF-Versionen des gesamten Handbuchs und einzelner Kapitel.

Ausdrucken dieses Handbuchs

Zum Ausdrucken dieses Handbuchs haben Sie entsprechend Ihren Anforderungen verschiedene Möglichkeiten.

- **Drucken einer Seite in der HTML-Ansicht**

  Jede Seite der HTML-Version des Handbuchs ist einem bestimmten Thema gewidmet. Verwenden Sie die Schaltfläche *Drucken* in der Symbolleiste des Browsers, um den Inhalt der Seite auszudrucken.

- **Drucken eines Kapitels**

  Verwenden Sie den Link *PDF-Datei dieses Kapitels* oben auf der Seite.

  – Klicken Sie auf den Link *PDF-Datei dieses Kapitels* oben rechts auf der Seite des Kapitels, das Sie ausdrucken möchten. Daraufhin wird die PDF-Version des jeweiligen Kapitels in einem Browser-Fenster geöffnet.

    Hinweis: Auf Ihrem Computer muss das kostenlose Programm Adobe Reader installiert sein, damit Sie PDF-Dateien öffnen und ausdrucken können. Sie erhalten dieses Programm auf der Adobe-Website unter *http://www.adobe.com*.

  – Klicken Sie auf das Symbol „Drucken“ oben links im Fenster.

    Tipp: Wenn Sie mit Ihrem Drucker zwei Seiten auf einem Blatt Papier ausdrucken können, sollten Sie diese Funktion auswählen, um Papier und Tinte zu sparen.

- **Drucken des gesamten Handbuchs**

  Verwenden Sie den Link *Gesamtes PDF-Handbuch* oben links auf der Seite.

  – Klicken Sie auf den Link *Gesamtes PDF-Handbuch* oben links auf der jeweiligen Handbuchseite. Daraufhin wird die PDF-Version des gesamten Handbuchs in einem Browser-Fenster geöffnet.
  – Klicken Sie auf das Symbol „Drucken“ oben links im Fenster.

    Tipp: Wenn Sie mit Ihrem Drucker zwei Seiten auf einem Blatt Papier ausdrucken können, sollten Sie diese Funktion auswählen, um Papier und Tinte zu sparen.

Kapitel 2
Einführung

Herzlichen Glückwunsch zum Kauf des NETGEAR® RangeMax Wireless Router WPN824. Der WPN824 Router ermöglicht die Anbindung mehrerer Computer an das Internet über ein externes Breitband-Zugangsgerät (z. B. ein Kabel- oder DSL-Modem), das normalerweise für einzelne Computer eingesetzt wird. In diesem Kapitel werden die Merkmale und Funktionen des NETGEAR RangeMax Wireless Router WPN824 beschrieben.

Die wichtigsten Merkmale

Hinweis: In diesem Handbuch finden Sie Informationen zu allen verfügbaren Funktionen zum Zeitpunkt der Drucklegung. Frühere Versionen dieses Produkts weisen möglicherweise nicht alle in diesem Handbuch vorgestellten Merkmale auf.

Der RangeMax Wireless Router WPN824 verfügt über einen Switch mit vier Ports und ermöglicht die Anbindung Ihres LANs (Local Area Network, Lokales Netz) an das Internet; dazu wird ein externes Zugangsgerät wie ein Kabel- oder DSL-Modem verwendet.

Der WPN824 Router bietet Ihnen verschiedene Optionen für die Content-Filterung im Internet sowie zur Protokollierung von Browsing-Vorgängen und sofortige Warnmeldungen per E-Mail. Eltern und Netzwerkadministratoren können den Zugriff nach Uhrzeit, Website-Adressen und Stichwörtern für Website-Adressen einschränken und für bis zu 253 Computer einen schnellen Internetzugang über Kabel-/DSL-Modem einrichten. Zusätzlich zur Netzwerk-Adressumsetzung (Network Address Translation, NAT) schützt Sie auch die integrierte Firewall vor Hackern.

Der Konfigurationsaufwand für den Router ist minimal – schon nach wenigen Minuten ist Ihr Gerät installiert und betriebsbereit.

Der WPN824 Router bietet folgende Leistungsmerkmale:

- MIMO-basierte RangeMax™-Technik (Multi-In, Multi-Out)
- Für drahtlose Netzwerke entsprechend 802.11g, auch kompatibel mit den Modi 802.11-Turbo-g oder 802.11b+g
- Einfache, webbasierte Installation und Verwaltung
- Größere Sicherheit durch Content-Filterung und Website-Sperrungen

- Integrierter 10/100-Switch mit vier Ports
- Netzwerkanschluss an ein WAN-Gerät (Wide Area Network, Fernnetz), z. B. ein Kabel- oder DSL-Modem
- Umfassende Unterstützung gängiger Protokolle
- Anmeldefunktion
- LEDs an der Vorderseite zur bequemen Kontrolle von Status und Betrieb
- Flash-Speicher für Firmware-Upgrades

MIMO-basierte RangeMax™-Technik (Multi-In, Multi-Out)

NETGEARs MIMO-basierte RangeMax™-Technik (Multi-In, Multi-Out) liefert durch Vermeidung von Funkschatten in dem Bereich, in dem Sie Ihre drahtlosen Computer benutzen, eine drastisch bessere Reichweite als der Standardmodus 802.11g. So wird Ihr ganzes Haus oder Ihr gesamter Bürokomplex zum „Hotspot“, ohne zusätzliche Erweiterungsschaltungen, Verstärker oder externe Antennen. RangeMax™ gewährt eine gleich bleibend schnelle Übertragung im ganzen Haus, nicht nur in der Nähe des Routers.

RangeMax™ ist eine erweiterte Smart MIMO-Technik (Multi-In, Multi-Out) mit sieben internen Antennen. RangeMax™ sucht Ihr Haus ständig nach physischen Hindernissen und Funkstörungen ab und passt das Funksignal an, um diese Leistungshemmer auszugleichen.

Wenn Sie z. B. Ihren Notebook vom Wohnzimmer ins Schlafzimmer tragen, erfasst RangeMax™ diese Veränderung automatisch und wählt aus mehr als 100 möglichen Antennenkonfigurationen die beste aus, um die schnellste, klarste Verbindung herzustellen. So profitieren alle Nutzer von gleich bleibend schnellen Verbindungen überall im Haus, ohne Leistungsgefälle und Funkschatten.

RangeMax™ ist außerdem hundertprozentig mit Ihren vorhandenen 802.11b/g-Produkten (also drahtlosen 802.11b-, 802.11g-, Centrino- und SuperG™-Clients) kompatibel und erhöht deren Reichweite und Übertragungsgeschwindigkeit um bis zu 50 %.

Drahtlose 802.11g-Netzwerke

In den WPN824 Router ist ein drahtloser 802.11g Access Point integriert, der eine kontinuierliche Hochgeschwindigkeitsverbindung mit bis zu 108 MBit/s zwischen drahtlosen Geräten und kabelgebundenen Netzwerkgeräten herstellt. Der Access Point hat folgende Merkmale:

- Drahtloser 802.11g-Netzwerkbetrieb mit bis zu 108 MBit/s
- Drahtloser Netzwerkbetrieb mit der Möglichkeit zum Betrieb in den Modi 802.11g, 802.11b oder 802.11g und b, d. h. Rückwärtskompatibilität mit 802.11b-Geräten oder Nutzung des drahtlosen Netzwerks mit den höheren Bandbreiten von 802.11g-Geräten
- Sicherheit durch 64-Bit und 128-Bit WEP-Verschlüsselung
- WEP-Schlüssel können manuell oder automatisch per Passphrase eingerichtet werden.

- WPA-PSK-Unterstützung: Unterstützung für WPA-Datenverschlüsselung für besondere Datensicherheit und Authentifizierung durch einen gemeinsamen Datenschlüssel
- Der drahtlose Zugriff kann über MAC-Adressen eingeschränkt werden.
- Die Ausstrahlung des Netzwerknamens kann ausgeschaltet werden, damit nur Geräte, die den Netzwerknamen (SSID) kennen, eine Verbindung herstellen können.

Leistungsstarke, echte Firewall mit Content-Filterung

Im Gegensatz zu einfachen, Internet-gestützten NAT-Routern ist der WPN824 eine echte Firewall, die Hackerangriffe über eine Stateful Packet Inspection (Paketüberprüfung) abwehrt. Leistungsmerkmale der Firewall:

- Schutz vor Denial of Service (DoS) -Attacken

  Erkennt und unterbindet DoS-Angriffe wie Ping of Death, SYN Flood, LAND Attack und IP-Spoofing automatisch
- Sperrt unerwünschten Datenverkehr aus dem Internet in Ihr LAN
- Sperrt den Zugriff von Ihrem LAN auf Websites oder Internet-Dienste, die Sie als unerwünscht angeben
- Führt ein Protokoll über sicherheitsrelevante Zwischenfälle

  Der WPN824 protokolliert sicherheitsrelevante Ereignisse wie gesperrte eingehende Datenübertragungen, Port-Abfragen, Angriffe und Anmeldungen durch den Administrator. Bei der Konfiguration des Routers können Sie festlegen, dass dieses Protokoll in bestimmten Abständen per E-Mail an Sie gesendet werden soll. Außerdem können Sie den Router so konfigurieren, dass bei einem wichtigen Ereignis sofort eine Benachrichtigung an Ihre E-Mail-Adresse oder Ihren E-Mail-Pager gesendet wird.
- Der WPN824 verhindert, dass fragwürdige Inhalte auf Ihre Computer gelangen. Den Zugriff auf Internet-Inhalte können Sie durch Prüfung von Stichwörtern in den Website-Adressen steuern. Bei der Konfiguration des Routers können Sie festlegen, dass Zugriffsversuche auf fragwürdige Websites protokolliert und gemeldet werden sollen.

Sicherheit

Der WPN824 Router verfügt über verschiedene Sicherheitsfunktionen, die in diesem Abschnitt beschrieben werden.

- Durch NAT geschützte Computer
  NAT (Network Address Translation, Netzwerk-Adressumsetzung) öffnet für Anfragen aus dem lokalen Netzwerk einen temporären Pfad ins Internet. Anfragen, die außerhalb des LANs gestartet wurden, werden gelöscht; dadurch wird verhindert, dass Benutzer außerhalb des LANs die zum LAN gehörigen Computer finden und auf sie zugreifen.

- Portweiterleitung mit NAT
  Obwohl NAT den direkten Zugriff von Internet-Adressen auf die Computer innerhalb des LANs verhindert, können Sie mit Hilfe des Routers die Weiterleitung eingehender Daten an einzelne Computer (entsprechend der Portnummer des Dienstes) oder an einen festgelegten „DMZ“-Host-Computer veranlassen. Diese Weiterleitung kann für einzelne Ports oder für Port-Bereiche definiert werden.

Netzwerkverbindungen mit automatischer Erkennung durch Auto Uplink

Mit dem internen 10/100-Switch mit vier Ports ermöglicht der WPN824 den Anschluss an ein Standard-Ethernet-Netzwerk mit 10 MBit/s oder an ein Fast-Ethernet-Netzwerk mit 100 MBit/s. Sowohl die LAN- als auch die WAN-Schnittstelle verfügen über eine automatische Erkennungsfunktion und unterstützen sowohl Vollduplex- als auch Halbduplex-Betrieb.

Der Router verwendet die Auto Uplink™-Technologie. Jeder Netzwerk-Port erkennt automatisch, ob das in den Port eingesteckte Netzwerkkabel eine „normale“ Verbindung, z. B. zu einem Computer, oder eine „Uplink“-Verbindung, z. B. zu einem Switch oder Hub, benötigt. Daraufhin wird der Anschluss automatisch für die erforderliche Verbindung konfiguriert. Damit können Sie auch auf Crossover-Kabel verzichten, da Auto Uplink in jedem Fall die richtige Verbindung für den jeweiligen Kabeltyp herstellt.

Umfassende Unterstützung gängiger Protokolle

Der WPN824 Router unterstützt das Transmission Control Protocol/Internet Protocol (TCP/IP) und das Routing Information Protocol (RIP). Weitere Informationen zu TCP/IP finden Sie in Anhang B, „Netzwerke, Routing, Firewalls und Grundlagen“.

- Gemeinsame Nutzung einer IP-Adresse durch NAT
  Mit dem WPN824 Router können mehrere Computer innerhalb eines Netzwerks einen gemeinsamen Internetzugang mit nur einer IP-Adresse nutzen, die von Ihrem Internetdienstanbieter (Internet Service Provider, ISP) statisch oder dynamisch zugewiesen wird. Dieses als NAT (Network Address Translation, Netzwerk-Adressumsetzung) bezeichnete Verfahren erlaubt die Verwendung eines kostengünstigen Internetzugangs für Einzelbenutzer.
- Automatische Konfiguration angeschlossener Computer durch DHCP
  Informationen zur Netzwerkkonfiguration, z. B. IP-, Gateway- und DNS-Adressen (Domain Name Server) werden den an das LAN angeschlossenen Computern durch den WPN824 Router dynamisch zugewiesen; dabei kommt die DHCP-Funktion (Dynamic Host Configuration Protocol) zum Einsatz. Diese Funktion vereinfacht die Konfiguration von Computern im lokalen Netzwerk beträchtlich.
- DNS-Proxy
  Wenn DHCP aktiviert ist und keine DNS-Adressen angegeben sind, stellt der Router den angeschlossenen Computern seine eigene Adresse als DNS-Server zur Verfügung. Während des Verbindungsaufbaus fragt der Router die tatsächlichen DNS-Adressen beim ISP ab und leitet DNS-Anfragen aus dem LAN weiter.

- PPP over Ethernet (PPPoE)
  PPPoE ist ein Protokoll für den Anschluss dezentraler Hosts an das Internet; dabei wird durch Simulation einer Wählverbindung eine DSL-Verbindung hergestellt. Diese Funktion macht die Ausführung eines Anmeldeprogramms wie Entersys oder WinPOET auf Ihrem Computer überflüssig.

Einfache Installation und Verwaltung

Nach Anschluss an das Netzwerk können Sie den RangeMax Wireless Router WPN824 innerhalb weniger Minuten installieren, konfigurieren und in Betrieb nehmen. Folgende Funktionen erleichtern Ihnen dabei die Installation und Verwaltung:

- Browser-basierte Verwaltung
  Mit der Browser-basierten Konfiguration können Sie Ihren Router von fast jedem Computer aus konfigurieren (z. B. Windows, Apple oder Linux). Dabei hilft Ihnen ein benutzerfreundlicher Setup-Assistent; darüber hinaus verfügt die Browser-basierte Web-Management-Benutzeroberfläche über eine integrierte Online-Hilfe.
- Smart Wizard
  Der Smart Wizard des WPN824 Routers erkennt automatisch den Typ der Internetverbindung und fordert von Ihnen nur die Informationen an, die für Ihren ISP-Internetzugang erforderlich sind.
- Firmware-Update
  Der WPN824 Router kann aktualisiert werden, wenn eine neuere Firmware-Version verfügbar ist. So können Sie Produktverbesserungen für Ihren WPN824 nutzen, sobald sie bereitgestellt werden.
- Überwachungsanzeigen
  Die LEDs an der Vorderseite des WPN824 Routers ermöglichen eine einfache Überwachung des Status und der Aktivität des Routers.

Wartung und Support

NETGEAR unterstützt Sie bei der optimalen Nutzung Ihres WPN824 Routers mit folgenden Funktionen:

- Flash-Speicher für Firmware-Upgrades
- Deutschsprachiger telefonischer Support (Montag bis Freitag zu normalen Bürozeiten, außer an Feiertagen)

Verwandte NETGEAR-Produkte

Die folgenden NETGEAR-Produkte passen zum RangeMax Wireless Router WPN824:

- RangeMax™ Wireless USB 2.0-Adapter (WPN111)
- RangeMax™ Wireless PCI-Adapter (WPN311)
- RangeMax™ Wireless PC-Card (WPN511)

Lieferumfang

In der Produktpackung sollten folgende Teile enthalten sein:

- RangeMax Wireless Router WPN824
- Netzteil
- Vertikalaufsteller
- CAT-5-Netzwerkkabel (Kategorie 5)
- *Ressourcen-CD für den NETGEAR RangeMax Wireless Router WPN824* mit folgendem Inhalt:
  - — Dieses Handbuch
  - — Anwendungshinweise und weitere hilfreiche Informationen
- *Setup-Anleitung für den Wireless Home Router*
- Karte mit Garantie- und Supportinformationen

Falls eines dieser Elemente fehlt, beschädigt oder das falsche Modell ist, wenden Sie sich bitte an Ihren NETGEAR-Fachhändler. Bewahren Sie den Karton sowie das Original-Verpackungsmaterial für den Fall auf, dass Sie den Router zu einem späteren Zeitpunkt zur Reparatur einsenden müssen.

Vorderseite des Routers

An der Vorderseite des WPN824 Routers befinden sich die unten beschriebenen Status-LEDs.

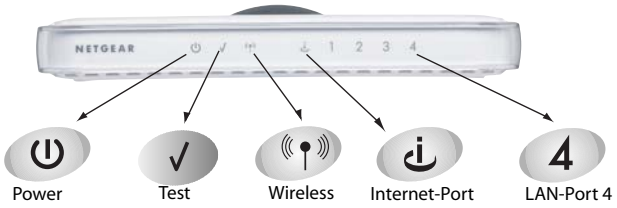


Abbildung 2-1: Vorderseite des WPN824

Anhand der Status-LEDs können Sie Verbindungen überprüfen. In der unten stehenden Tabelle werden die LEDs an der Vorderseite des Routers von links nach rechts beschrieben.

Tabelle 2-1. Beschreibung der Status-LEDs

Symbol	Zustand	Beschreibung
Power	Leuchtet grün	Der Router ist an die Netzversorgung angeschlossen und hat den Diagnosetest bestanden.
	Aus	Der Router ist nicht an die Netzversorgung angeschlossen.
Test	Ein	Das Gerät führt den Selbsttest zum Systemstart durch.
	Aus	Das Gerät hat den Selbsttest zum Systemstart erfolgreich abgeschlossen.
Wireless	Ein	Der Access Point ist initialisiert und die Wireless-Funktion aktiviert.
	Aus	Die Wireless-Funktion ist ausgeschaltet oder es ist ein Problem aufgetreten.
Internet	Ein	Der Internet-Port hat eine Verbindung zu einem angeschlossenen Gerät erkannt.
	Blinkt	Daten werden über den Internet-Port übertragen oder empfangen.
LAN	Ein (Grün)	Der LAN-Port hat eine Verbindung mit 100 MBit/s zu einem angeschlossenen Gerät erkannt.
	Blinkt (Grün)	Daten werden mit 100 MBit/s übertragen oder empfangen.
	Ein (Gelb)	Der lokale Port hat eine Verbindung mit 10 MBit/s zu einem angeschlossenen Gerät erkannt.
	Blinkt (Gelb)	Daten werden mit 10 MBit/s übertragen oder empfangen.
	Aus	An diesem Port wurde keine Verbindung erkannt.

Rückseite des Routers

An der Rückseite des WPN824 befinden sich die unten beschriebenen Elemente.

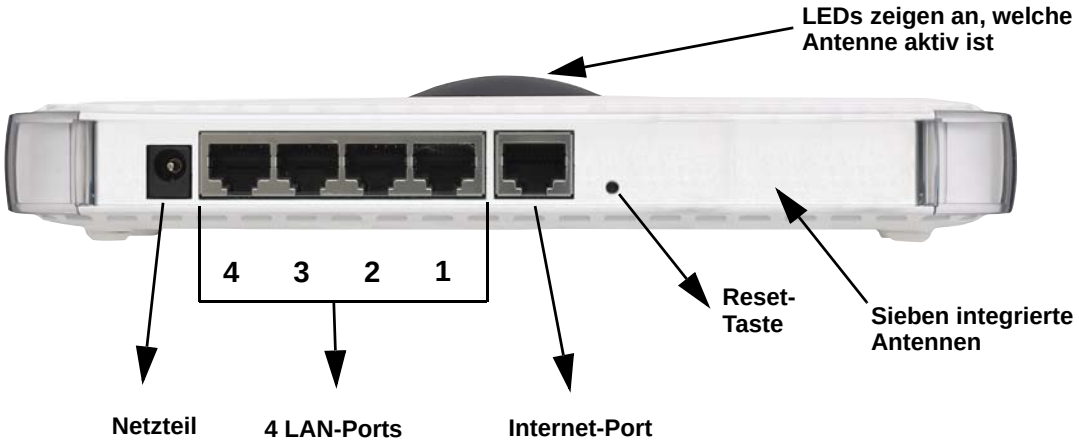


Abbildung 2-2: Rückseite des WPN824

Von links nach rechts finden Sie an der Rückseite die folgenden Elemente:

- Netzanschluss für 12 V bei 1 A Ausgangsstrom, max. 22 W
- Vier lokale (LAN-) 10/100 MBit/s-Ports für den Anschluss des Routers an lokale Computer
- Internet- (WAN-) Port für den Anschluss des Routers an ein Kabel- oder DSL-Modem
- Reset-Taste zum Wiederherstellen von Werkseinstellungen und Passwort

Eine Übersicht für den „Weg zum Erfolg“

Die Einführung neuer Technologien kann sich schwierig gestalten. Breitband-Internetdienste werden inzwischen als so vorteilhaft angesehen, dass immer mehr Anwender Netzwerke zu Hause einrichten wollen, um eine Breitbandverbindung gemeinsam zu nutzen. Durch die drahtlose Netzwerktechnik gibt es dabei ein Problem weniger – sie kommt ohne Kabel aus. Einerseits erhalten dadurch mehr Menschen Gelegenheit, Netzwerke zu nutzen, andererseits müssen sie dabei die komplexen Vorgänge in Netzwerken verstehen lernen. Das Netzwerkkonzept an sich, die Einrichtung und Wartung können schwer nachvollziehbar sein. Außerdem kommen durch die drahtlose Übertragung noch Aspekte wie Reichweite, Störungen, Signalstärke und Sicherheit ins Spiel.

Um mögliche Hindernisse bei der erfolgreichen Einrichtung eines Heimnetzwerks zu beseitigen, können Sie an der unten stehenden Tabelle ablesen, wie Sie eine Verbindung zu einem drahtlosen Netzwerk (WLAN) herstellen, für die nötigen Sicherheitsmaßnahmen sorgen, über die drahtlose Verbindung ins Internet gehen, Dateien mit anderen Computern austauschen und Drucker in einem Netzwerk aus drahtlosen und kabelgebundenen Geräten verwenden.

Tabelle 2-2. Eine Übersicht für den „Weg zum Erfolg“

Mein Ziel:	Was muss ich tun?	Was brauche ich?	Wie geht das?
Ein drahtloses Netzwerk einrichten	1. Den RangeMax Wireless Router WPN824 einrichten 2. Den Netzwerknamen (SSID) für das WLAN und ggf. die Wireless-Sicherheits-einstellungen ermitteln 3. Die drahtlosen Computer mit den Einstellungen aus Schritt 1 einrichten	• Ein drahtloses Netzwerk • Einen Computer innerhalb der effektiven Reichweite des WLAN. Richtlinien zur Reichweite drahtloser Netzwerke finden Sie unter „Hinweise zur Leistung, Aufstellung und Reichweite“ auf Seite 4-1.	Befolgen Sie zur Einrichtung des WPN824 die Anleitungen in Kapitel 3, „Verbindung des Routers mit dem Internet“. Eine allgemeine Einführung in die drahtlose Netzwerktechnik finden Sie in Anhang 4, „WLAN-Konfiguration“.

Tabelle 2-2. Eine Übersicht für den „Weg zum Erfolg“ (Fortsetzung)

Mein Ziel:	Was muss ich tun?	Was brauche ich?	Wie geht das?
Meine Wireless-Verbindung vor fremden Augen, Hackern oder Datendiebstahl **schützen**	1. Sicherstellen, dass die Sicherheitsfunktionen für das WLAN aktiviert sind 2. Meinen WPN824 mit den Sicherheits-einstellungen des WLAN konfigurieren 3. Die Windows-Sicherheits-funktionen nutzen	• Ein WLAN mit WEP- oder WPA-Sicherheitsfunktion • WLAN-Geräte, die WEP oder WPA unterstützen, wie der WPN824	Informationen zur Sicherheit drahtloser Netzwerke finden Sie unter „Grundlagen drahtloser Netzwerke“ auf Seite D-1. Lesen Sie unter „Angemessene Sicherheitsmaßnahmen für Ihr drahtloses Netzwerk“ auf Seite 4-2 zu Sicherheitsfunktionen nach und konfigurieren Sie Ihren WPN824 entsprechend.
Hinweis: Sichere Websites wie die von Banken und Online-Händlern nutzen Verschlüsselungsfunktionen, die in Browser wie Internet Explorer und Netscape integriert sind. Alle von Ihnen eingerichteten Sicherheitsfunktionen für drahtlose Netzwerke ergänzen die bereits auf sicheren Websites vorhandenen Funktionen.			
Windows PC-Dateien und -Drucker zu Hause in einem kombinierten drahtlosen und verdrahteten Netzwerk **gemeinsam nutzen** **Hinweis:** Wenn Sie Dateien und Drucker auf Computern mit anderen Betriebssystemen, wie Mac OS oder Linux, gemeinsam nutzen möchten, lesen Sie dazu die Bedienungsanleitung für das jeweilige Betriebssystem.	1. Verwenden Sie die Windows Drucker- und Fax-Einstellungen, um freigegebene Drucker im Netzwerk zu finden. 2. Verwenden Sie den Windows-Drucker-installations-assistenten, um von Ihrem drahtlos ver-bundenen PC auf einen im Netzwerk freigegebenen Drucker zuzugreifen. 3. Verwenden Sie in Ihren Anwendungen unter dem Menüpunkt „Drucken“ die Druckerauswahl, um die Ausgabe auf einen Netzwerkdrucker zu leiten.	• Auf Windows-Computern, die im Netzwerk (kabelgebunden oder drahtlos) verwendet werden, müssen der „Client für Microsoft-Netzwerke“ sowie die „Datei- und Druckerfreigabe“ eingerichtet sein. • Windows-Computer (kabelgebunden oder drahtlos), die für den Netzwerkanschluss verwendet werden, müssen dieselben Arbeitsgruppen- oder Domänen-Einstellungen erhalten wie die anderen Computer im Netzwerk. • Alle durch Windows für Freigaben festgelegten Benutzernamen/ Passwörter müssen nach Aufforderung eingegeben werden. • Wenn ein Windows-Netzwerk verwendet wird, müssen Drucker zur gemeinsamen Nutzung erst freigegeben werden.	Windows-Domänen werden normalerweise von gewerblichen Systembetreuern eingerichtet. Windows-Arbeitsgruppen werden von Nutzern eingerichtet, die kleine Netzwerke zu Hause oder in einer kleinen Firma verwenden. Hilfe zur Einrichtung von Windows-Netzwerken erhalten Sie im Tutorial für PC-Netzwerke auf der *Ressourcen-CD für den NETGEAR RangeMax Wireless Router WPN824* und in den Hilfe-Texten für das von Ihnen verwendete Windows-System. Hilfe zur Einrichtung von Druckern unter Windows erhalten Sie in den Hilfe- und Support-Informationen zu Ihrer Version des Windows-Betriebssystems.

Kapitel 3
Verbindung des Routers mit dem Internet

In diesem Kapitel wird beschrieben, wie Sie den Router in Ihrem Local Area Network (LAN) einrichten und ihn mit dem Internet verbinden. Sie erfahren, wie Sie Ihren RangeMax Wireless Router WPN824 mit dem Setup-Assistenten für den Internetzugriff konfigurieren oder Ihre Internetverbindung manuell konfigurieren.

Befolgen Sie die nachstehenden Anleitungen, um Ihren Router einzurichten.

Vorbereitung der Installation Ihres Wireless Routers

- Beachten Sie die Hinweise zur Aufstellung und Reichweite von drahtlosen Geräten unter „Hinweise zur Leistung, Aufstellung und Reichweite“ auf Seite 4-1.
- *Beim Einsatz mit einem Kabelmodem*: Verwenden Sie zum Einrichten des Wireless Routers unbedingt den Computer, auf dem Sie sich ursprünglich bei Ihrem Kabeldienstanbieter registriert haben.
- *Beim Einsatz mit DSL*: Zum Einrichten des Wireless Routers benötigen Sie u. U. Anmeldedetails für die DSL-Verbindung, wie Benutzernamen/E-Mail-Adresse und Passwort.

Vor der Installation des Wireless Routers sollten Sie sich die *Ressourcen-CD für den NETGEAR RangeMax Wireless Router WPN824* ansehen, vor allem dieses Handbuch und die Tutorials zur Netzwerkkonfiguration von PCs.

Konfigurieren Sie den Wireless Router zunächst mit dem Smart Wizard

Legen Sie die *Ressourcen-CD* in das CD-Laufwerk Ihres PCs ein. Daraufhin wird der folgende Bildschirm angezeigt. Klicken Sie auf **Setup** und befolgen Sie die Aufforderungen.

Abbildung 3-1: Installationsassistent NETGEAR Smart Wizard

Richten Sie jetzt einen Computer für drahtlose Verbindungen ein

Sie sind jetzt mit dem Internet verbunden und die Wireless-Funktion des Wireless Routers ist aktiviert! Konfigurieren Sie nun Ihren drahtlosen Computer.

1. Konfigurieren der Einstellungen für den Wireless-Adapter Ihres Computers

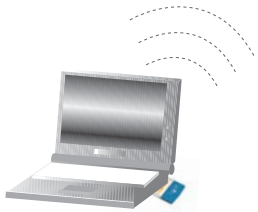


Abbildung 3-2: Konfigurieren des drahtlosen Computers

Wireless-Adapter von NETGEAR, Inc. zeigen eine Liste der verfügbaren drahtlosen Netzwerke an. Wählen Sie bei deaktivierten Sicherheitsmaßnahmen für drahtlose Netzwerke einfach Ihr Netzwerk aus der Liste und stellen Sie die Verbindung her.

Wireless-Adapter, die nicht von NETGEAR stammen, müssen so eingerichtet werden, dass sie genau Ihren Einstellungen entsprechen. Wenn Sie den Standard-Netzwerknamen (SSID) geändert haben, verwenden Sie unbedingt den richtigen Netzwerknamen (SSID), den Sie im Wireless Router festgelegt haben.

WIRELESS-FUNKTION	STANDARDEINSTELLUNG
Netzwerkname (SSID)	**NETGEAR**
WEP-Verschlüsselung	**Deaktiviert**

Warnung: Bei Netzwerknamen (SSID) wird zwischen Groß- und Kleinschreibung unterschieden. (Geben Sie also z. B. nicht „nETgear“ ein.)

2. Überprüfen der drahtlosen Verbindung

Überprüfen Sie die drahtlose Verbindung. Verwenden Sie einen Computer mit einem Wireless-Adapter, um eine Verbindung zum Internet herzustellen oder sich beim Wireless Router anzumelden. Probleme mit drahtlosen Verbindungen werden unter „Tipps zur Fehlerbehebung“ auf Seite 3-4 behandelt.

Sie sind jetzt drahtlos mit dem Internet verbunden! Stellen Sie die Sicherheitsoptionen für Ihre drahtlose Verbindung entsprechend der Anleitung in „Angemessene Sicherheitsmaßnahmen für Ihr drahtloses Netzwerk“ auf Seite 4-2 ein.

Tipps zur Fehlerbehebung

Hier finden Sie Tipps zur Behebung einfacherer Probleme.

Achten Sie beim Neustart Ihres Netzwerks auf die Einhaltung dieser Reihenfolge:

1) Schalten Sie das Modem, den Wireless Router und den Computer aus. 2) Schalten Sie das Modem ein und warten Sie zwei Minuten. 3) Schalten Sie den Wireless Router ein und warten Sie eine Minute. 4) Schalten Sie den Computer ein.

Überprüfen Sie, ob die Netzwerkkabel richtig angeschlossen sind.

- Die Internet-Statusanzeige des Wireless Routers leuchtet, wenn das Netzwerkkabel ordnungsgemäß mit dem Modem und dem Wireless Router verbunden ist und Modem und Wireless Router eingeschaltet sind.
- Für jeden eingeschalteten Computer, der über ein ordnungsgemäß eingestecktes Netzwerkkabel mit dem Wireless Router verbunden ist, leuchtet die entsprechende LAN-Port-Statusanzeige am Wireless Router auf. Die Nummern der einzelnen LAN-Ports entnehmen Sie bitte dem Etikett auf der Unterseite des Wireless Routers.

Vergewissern Sie sich, dass die Drahtloseinstellungen auf dem Computer und dem Router identisch sind.

Der Name des drahtlosen Netzwerks (SSID) und die WEP-/WPA-Einstellungen des Routers und des drahtlos verbundenen Computers müssen identisch sein.

Vergewissern Sie sich, dass die Netzwerkeinstellungen des Computers korrekt sind.

- Über LAN oder drahtlos verbundene Computer *müssen* so konfiguriert sein, dass die IP-Adresse automatisch über DHCP bezogen wird. Hilfe hierzu finden Sie unter Anhang C, „Netzwerkeinrichtung“ oder in den Tutorials auf der CD.
- Bei manchen Kabelmodem-Internetanbietern müssen Sie die MAC-Adresse des Computers verwenden, der für das Konto registriert ist. Ist dies der Fall, wählen Sie im Bereich „MAC-Adresse des Routers“ im Menü „Grundeinstellungen“ die Option **MAC-Adresse des Computers verwenden**. Der Router erfasst und verwendet dann die MAC-Adresse des derzeit benutzten Computers. Verwenden Sie also den Computer, der beim Internetanbieter registriert ist. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern. Starten Sie das Netzwerk in der richtigen Reihenfolge neu.

Überprüfen Sie anhand der Statusanzeige, ob der Router richtig konfiguriert ist.

- Wenn die Stromanzeige nicht innerhalb von 2 Minuten nach Einschalten des Routers grün wird, setzen Sie den Router zurück, wie unter „Wiederherstellen von Werkseinstellungen und Passwort“ auf Seite 7-7 beschrieben.
- Wenn die Wireless-Anzeige nicht aufleuchtet, überprüfen Sie, ob die Wireless-Funktion aktiviert ist, wie unter „Erläuterung der WLAN-Einstellungen“ auf Seite 4-4 beschrieben.

Überblick über die Zugriffsmöglichkeiten auf den Wireless Router

In der folgenden Tabelle sehen Sie, wie Sie je nach Zustand des Wireless Routers auf den Wireless Router zugreifen können.

Tabelle 3-1. Zugriffsmöglichkeiten auf den Router

Zustand des Routers	Zugriffsmöglichkeiten	Beschreibung
Werkseitige Voreinstellungen **Hinweis**: Der Wireless Router wird mit werkseitigen Voreinstellungen geliefert. Diese können auch durch Betätigen der Reset-Taste wiederhergestellt werden. Weitere Informationen zu dieser Funktion finden Sie unter „Wiederherstellen von Werkseinstellungen und Passwort“ auf Seite 7-7.	Automatischer Zugriff über den Konfigurations-assistenten Smart Wizard	Immer wenn auf einem Computer, der mit dem Wireless Router verbunden ist, ein Browser geöffnet wird, stellt der Wireless Router automatisch die Verbindung zu diesem Browser her und öffnet die Begrüßungsseite des Konfigurationsassistenten. Dazu müssen weder die URL des Wireless Routers im Browser eingegeben, noch der Benutzername oder das Passwort für die Anmeldung verwendet werden.
	Manuelle Eingabe einer URL zur Umgehung des Konfigurations-assistenten Smart Wizard	Sie können den Konfigurationsassistenten Smart Wizard umgehen, indem Sie in der Adressleiste des Browsers *http://www.routerlogin.net/basicsetting.htm* eingeben und die **Eingabetaste** drücken. Einen Benutzernamen oder ein Passwort brauchen Sie nicht einzugeben. Auf diese Weise können Sie den Wireless Router trotz der werkseitigen Voreinstellungen manuell konfigurieren. Wenn Sie den Router manuell konfigurieren, müssen Sie die Konfiguration durch Klicken auf „Übernehmen“ abschließen, wenn Sie alle Einstellungen eingegeben haben. Andernfalls wird auf dem Browser jedes PC, der mit dem Router verbunden ist, automatisch statt der Startseite des Browsers die Begrüßungsseite des Konfigurationsassistenten für den Router geöffnet.
Konfigurations-einstellungen wurden übernommen	Eingabe der Standard-URL für den Zugriff auf den Wireless Router	Stellen Sie die Verbindung zum Wireless Router her, indem Sie eine dieser URLs in die Adresszeile Ihres Browsers eingeben und die **Eingabetaste** drücken: • *http://www.routerlogin.net* • *http://www.routerlogin.com* Sie werden vom Wireless Router aufgefordert, den Benutzernamen **admin** und das Passwort einzugeben. Das Standardpasswort lautet **password**.
	Eingabe der IP-Adresse des Wireless Routers für den Zugriff auf den Wireless Router	Stellen Sie die Verbindung zum Wireless Router her, indem Sie die IP-Adresse des Wireless Routers in die Adresszeile Ihres Browsers eingeben und dann die **Eingabetaste** drücken. 192.168.1.1 ist die Standard-IP-Adresse des Wireless Routers. Sie werden vom Wireless Router aufgefordert, den Benutzernamen **admin** und das Passwort einzugeben. Das Standardpasswort lautet **password**.

So melden Sie sich nach dem Übernehmen der Konfigurationseinstellungen beim Wireless Router an

1. Stellen Sie die Verbindung zum Wireless Router her, indem Sie *http://www.routerlogin.net* in die Adresszeile Ihres Browsers eingeben und dann die **Eingabetaste** drücken.

Abbildung 3-3: Adresse für die Anmeldung

2. Aus Sicherheitsgründen sind für den Router ein eigener Benutzername und ein Passwort erforderlich. Geben Sie nach der Aufforderung als Benutzernamen für den Router **admin** und als Passwort **password** ein. Achten Sie darauf, beide Wörter klein zu schreiben. Unter „Ändern des Administratorpassworts“ auf Seite 6-9 können Sie nachlesen, wie das Passwort geändert wird.

   Hinweis: Der Benutzername und das Passwort für den Router unterscheiden sich von dem Benutzernamen und Passwort für die Internetverbindung.

Abbildung 3-4: Anmeldefenster

Nach der Eingabe Ihres Benutzernamens und Passworts sollte Ihr Webbrowser den WPN824 Router finden und die unten abgebildete Startseite anzeigen.

Abbildung 3-5: Ergebnis der Anmeldung: Die Startseite des WPN824

Der Browser zeigt nun die Startseite mit den Grundeinstellungen des WPN824 an.

Wenn der Wireless Router mit dem Internet verbunden ist, klicken Sie auf die Links **Online-Wissensdatenbank** oder **Dokumentation** im Menü „Support im Internet“, um Support-Informationen bzw. die Dokumentation für den Wireless Router anzuzeigen.

Wenn Sie nicht auf **Abmelden** klicken, wartet der Wireless Router fünf Minuten ab, ob eine Aktivität stattfindet, und führt dann automatisch die Abmeldung durch.

So umgehen Sie den Konfigurationsassistenten

1. Wenn die werkseitigen Voreinstellungen für den Wireless Router aktiviert sind, geben Sie *http://www.routerlogin.net/basicsetting.htm* in die Adresszeile Ihres Browsers ein und drücken Sie die **Eingabetaste**.

   Solange die werkseitigen Voreinstellungen für den Wireless Router gelten, ist kein Benutzername und kein Passwort erforderlich.

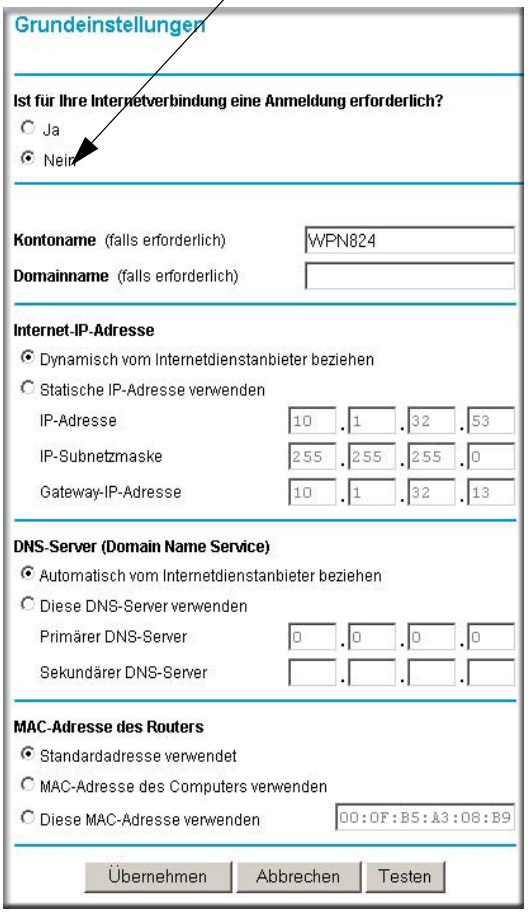
2. Der Browser zeigt nun die unter „Ergebnis der Anmeldung: Die Startseite des WPN824“ auf Seite 3-7 abgebildete Startseite mit den Einstellungen des WPN824 an.

   Wenn Sie nicht auf **Abmelden** klicken, wartet der Wireless Router fünf Minuten ab, ob eine Aktivität stattfindet, und führt dann automatisch die Abmeldung durch.

So konfigurieren Sie Ihre Internetverbindung manuell

Sie können Ihren Router über das unten abgebildete Menü manuell konfigurieren oder die Konfiguration vom Setup-Assistenten vornehmen lassen, wie im vorigen Abschnitt beschrieben.

Keine* Anmeldung beim ISP *erforderlich



Anmeldung beim ISP *erforderlich*

Abbildung 3-6: Browser-basierte Konfigurationsmenüs „Grundeinstellungen“

Sie können den Router mit den folgenden Schritten über das in Abbildung 3-6 gezeigte Menü „Grundeinstellungen“ manuell konfigurieren:

1. Stellen Sie die Verbindung zum Wireless Router her, indem Sie *http://www.routerlogin.net* in die Adresszeile Ihres Browsers eingeben und dann die **Eingabetaste** drücken.

2. Aus Sicherheitsgründen sind für den Wireless Router ein eigener Benutzername und ein Passwort erforderlich. Geben Sie nach der Aufforderung als Benutzernamen für den Router **admin** und als Passwort **password** ein. Achten Sie darauf, beide Wörter klein zu schreiben.
3. Klicken Sie im Konfigurationsmenü auf **Grundeinstellungen**.
4. Wenn für Ihre Internetverbindung keine Anmeldung erforderlich ist, klicken Sie oben im Menü „Grundeinstellungen“ auf **Nein** und geben Sie die Einstellungen entsprechend der folgenden Anleitung ein. Wenn für Ihre Internetverbindung eine Anmeldung erforderlich ist, klicken Sie auf **Ja** und gehen Sie weiter zu Schritt 5.
   a. Geben Sie Ihren Kontonamen (er kann auch als Hostname bezeichnet werden) und den Domainnamen ein.
   Diese Parameter können erforderlich sein, um auf Dienste Ihres ISP, wie Mail- oder Nachrichtenserver, zuzugreifen.
   b. **Internet-IP-Adresse**:
   Wenn Ihr ISP Ihnen eine permanente, feste (statische) IP-Adresse für Ihren Computer zugewiesen hat, wählen Sie **Statische IP-Adresse verwenden**. Geben Sie die **IP-Adresse** ein, die Ihr ISP Ihnen zugewiesen hat. Geben Sie auch die **IP-Subnetzmaske** und die **Gateway-IP-Adresse** ein. Das Gateway ist der Router des ISP, zu dem Ihr Router Verbindung aufnimmt.
   c. **DNS-Server (Domain Name Service)**:
   Wenn Sie wissen, dass Ihr ISP während der Anmeldung DNS-Adressen nicht automatisch an den Router überträgt, wählen Sie **Diese DNS-Server verwenden** und geben Sie die IP-Adresse für den **Primären DNS-Server** ein. Wenn es eine Adresse für einen **Sekundären DNS-Server** gibt, geben Sie diese ein.

   Hinweis: Wenn Sie hier eine Adresse eingeben, müssen Sie die Computer in Ihrem Netzwerk neu starten, damit die Einstellungen in Kraft treten.
   d. **MAC-Adresse des Routers**:
   In diesem Bereich wird die MAC-Adresse festgelegt, die der Router am Internet-Port verwendet. Manche Internetdienstanbieter (ISPs) registrieren die MAC-Adresse der Netzwerkkarte bei der Einrichtung Ihrer Internetverbindung in Ihrem Computer. Danach akzeptieren sie nur Datenverkehr von der MAC-Adresse dieses Computers. Mit dieser Funktion kann sich Ihr Router als dieser Computer ausgeben, indem er die MAC-Adresse kopiert.

   Wählen Sie zum Ändern der MAC-Adresse **MAC-Adresse des Computers verwenden**. Der Router erfasst und verwendet dann die MAC-Adresse des Computers, den Sie gerade benutzen. Verwenden Sie also den Computer, der beim ISP zugelassen ist. Oder wählen Sie **Diese MAC-Adresse verwenden** und geben Sie sie hier ein.
   e. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.
5. Wenn für Ihre Internetverbindung eine Anmeldung erforderlich ist, geben Sie die Einstellungen entsprechend der folgenden Anleitung ein. Wählen Sie **Ja**, wenn Sie normalerweise ein Anmeldeprogramm wie Enternet oder WinPOET starten müssen, um auf das Internet zuzugreifen.

Hinweis: Wenn Sie Ihren Router eingerichtet haben, brauchen Sie das Anmeldeprogramm Ihres ISPs nicht mehr zu starten, um auf das Internet zuzugreifen. Beim Start einer Internetanwendung meldet Ihr Router Sie automatisch an.

a. Wählen Sie Ihren **Internetdienstanbieter** (Internet Service Provider) aus der Dropdown-Liste.

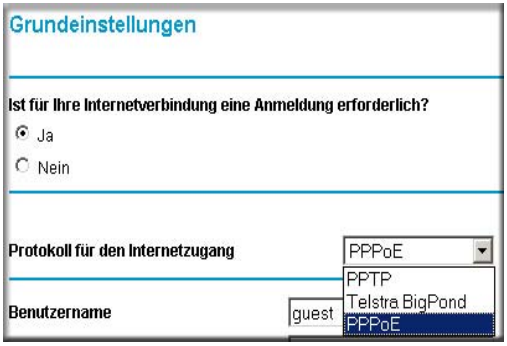


Abbildung 3-7: ISP-Liste in den Grundeinstellungen

Hinweis: Nicht alle Internetdienstanbieter sind hier aufgeführt. Für die Anbieter in dieser Liste gelten besondere Anforderungen.

b. Der Bildschirm wechselt je nach den für Ihren ISP erforderlichen Einstellungen.

c. Tragen Sie die Parameter für Ihren Internetdienstanbieter ein.

d. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern. Klicken Sie auf die Schaltfläche **Test**, um sicherzustellen, dass Sie Internetzugriff haben.

	Hinweis: Schenken Sie dem Feld „Leerlaufzeit“ besondere Beachtung, wenn Sie einen Internettarif mit Abrechnung auf Minutenbasis verwenden. Der Router trennt die Internetverbindung nur, wenn innerhalb der hier eingestellten Zeit keine Daten übertragen werden. Dies geschieht jedoch häufig auch unbemerkt, wenn z. B. automatische Updates aktiv sind oder E-Mail-Programme nach Post sehen. Stellen Sie den Wert nicht auf „0“, denn dies zieht eine permanente Verbindung nach sich. NETGEAR empfiehlt deshalb dringend den Abschluss von „Flatrates“ oder Tarifen auf Volumenbasis. NETGEAR wird keine Schäden ersetzen, die aufgrund erhöhter Internet-Rechnungen entstehen.

Verwendung des Setup-Assistenten

Sie können den Setup-Assistenten als Hilfestellung bei der manuellen Konfiguration oder zur Überprüfung der Internetverbindung verwenden. Der Setup-Assistent ist anders als der Konfigurationsassistent Smart Wizard (siehe Abbildung 3-1), der nur erscheint, wenn die werkseitigen Voreinstellungen des Routers eingestellt sind. Nach der Konfiguration des Wireless Routers taucht der Konfigurationsassistent Smart Wizard nicht wieder auf.

Befolgen Sie die nachstehende Anleitung, um den Setup-Assistenten als Hilfestellung bei der manuellen Konfiguration oder zur Überprüfung der Internetverbindung zu verwenden.

1. Stellen Sie die Verbindung zum Wireless Router her, indem Sie *http://www.routerlogin.net* in die Adresszeile Ihres Browsers eingeben und dann die **Eingabetaste** drücken.
2. Aus Sicherheitsgründen sind für den Router ein eigener Benutzername und ein Passwort erforderlich. Geben Sie nach der Aufforderung als Benutzernamen für den Router **admin** und als Passwort **password** ein. Achten Sie darauf, beide Wörter klein zu schreiben. Unter „Ändern des Administratorpassworts“ auf Seite 6-9 können Sie nachlesen, wie das Passwort geändert wird.

   Hinweis: Der Benutzername und das Passwort für den Router unterscheiden sich von dem Benutzernamen und Passwort für die Internetverbindung.

   Nach der Eingabe Ihres Benutzernamens und Passworts sollte der Webbrowser den WPN824 Router finden und die Startseite anzeigen, wie in „Ergebnis der Anmeldung: Die Startseite des WPN824“ auf Seite 3-7 beschrieben.
3. Klicken Sie oben links im Hauptmenü auf **Setup-Assistent**.
4. Klicken Sie zum Fortfahren auf **Weiter**. Geben Sie die Einstellungen für Ihren Internetanschluss ein.
5. Klicken Sie am Ende des Setups auf die Schaltfläche **Test**, um Ihre Internetverbindung zu überprüfen. Wenn Sie Probleme mit dem Einrichten der Internetverbindung haben, sehen Sie in den „Tipps zur Fehlerbehebung“ auf Seite 3-4 nach, um grundlegende Probleme zu beheben, oder lesen Sie Kapitel 7, „Fehlerbehebung“.

NETGEAR Produktregistrierung, Support und Dokumentation

Registrieren Sie Ihr Produkt unter *http://www.netgear.de/registrierung*. Die Registrierung ist Voraussetzung für die Nutzung unseres telefonischen Supports.

Wenn der Wireless Router mit dem Internet verbunden ist, klicken Sie auf die Links **Online-Wissensdatenbank** oder **Dokumentation** im Menü „Support im Internet“, um Support-Informationen bzw. die Dokumentation für den Wireless Router anzuzeigen.

Kapitel 4
WLAN-Konfiguration

In diesem Kapitel erfahren Sie, wie Sie die drahtlosen Eigenschaften Ihres WPN824 Routers konfigurieren. Bei der Planung Ihres drahtlosen Netzwerks sollten Sie die erforderliche Sicherheitsstufe bedenken. Außerdem sollten Sie Ihre Firewall optimal platzieren, um eine möglichst hohe Übertragungsrate für das Netzwerk zu erreichen. Weitere Informationen zum drahtlosen Netzwerkbetrieb finden Sie in Anhang D, „Grundlagen drahtloser Netzwerke“.

Hinweise zur Leistung, Aufstellung und Reichweite

Die Reichweite Ihrer drahtlosen Verbindung hängt stark davon ab, wo Sie die Wireless Firewall aufstellen. Die Latenzzeit, Datendurchsatzleistung und der Stromverbrauch von Wireless-Adaptern sind auch von den Konfigurationseinstellungen abhängig.

Hinweis: Ein ordnungsgemäßer und störungsfreier Betrieb des Routers bei voller Leistung ist nur gewährleistet, wenn die entsprechenden Hinweise beachtet werden. Vollständige Daten zur Reichweite/Leistung finden Sie in Anhang A, „Technische Daten“.

Berücksichtigen Sie bei der Wahl des Standorts für Ihre Firewall die folgenden Hinweise:

- Eine möglichst zentrale Platzierung in dem Bereich, in dem die Computer eingesetzt werden.
- Erhöhte Position (z. B. oben auf einem Regal), damit der Router „Sichtverbindungen“ zu den drahtlos verbundenen Computern herstellen kann (ggf. auch durch Wände).
- Entfernt von Störquellen wie Computern, Mikrowellengeräten und schnurlosen DECT-Telefonen.
- Nicht in der Nähe von großen Metallflächen.

Die Zeit, die zum Aufbau einer drahtlosen Verbindung benötigt wird, hängt von den Sicherheitseinstellungen und der Aufstellung des Geräts ab. Der Aufbau von WEP-Verbindungen dauert etwas länger. Außerdem kann WEP- und WPA-PSK-Verschlüsselung zu erhöhtem Stromverbrauch auf Notebook-Computern führen.

Auf Metallflächen sollten MIMO-Geräte vertikal aufgestellt werden, damit ein störungsfreier Betrieb gewährleistet ist. Alternativ kann der Router jedoch auch – z. B. durch einen darunter stehenden Karton – von der Metalloberfläche abgehoben werden.

Abbildung 4-1: Vertikale Aufstellung auf Metallflächen sinnvoll

Angemessene Sicherheitsmaßnahmen für Ihr drahtloses Netzwerk

	Hinweis: In geschlossenen Räumen können Computer in einem enormen Radius an drahtlose 802.11b/g-Netzwerke angeschlossen werden. Bei derartigen Entfernungen ist es möglich, dass auch Dritte außerhalb Ihres unmittelbaren Bereichs sich Zugang zu Ihrem Netzwerk verschaffen.

Anders als bei kabelgebundenen Netzwerken können drahtlos übertragene Daten auch von außerhalb empfangen werden, wenn der Betreffende über einen kompatiblen Adapter verfügt. Nutzen Sie also die Sicherheitsfunktionen Ihrer Wireless-Ausrüstung. Der WPN824 Router bietet sehr effektive Sicherheitsfunktionen, die in diesem Kapitel ausführlich beschrieben werden. Setzen Sie die für Ihre Anforderungen geeigneten Sicherheitsfunktionen ein.

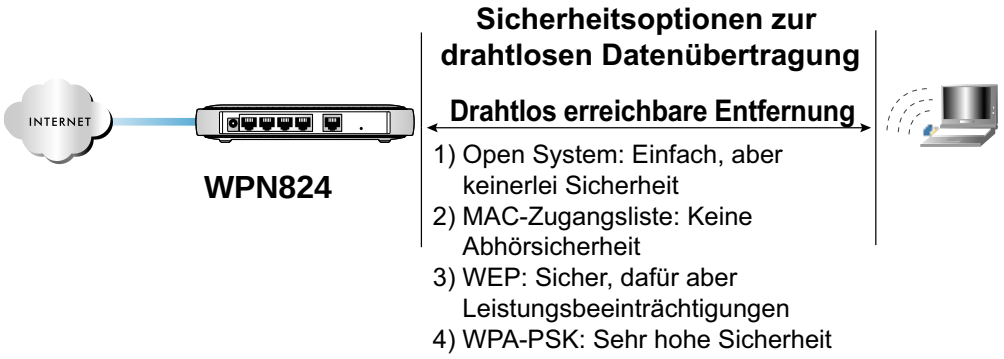


Abbildung 4-2: WPN824 Sicherheitsoptionen zur drahtlosen Datenübertragung

Es gibt mehrere Möglichkeiten, die Sicherheit Ihres drahtlosen Netzwerks zu verbessern.

- **Beschränken Sie den Zugang anhand von MAC-Adressen.** Sie können den Zugang auf bekannte Computer beschränken, damit unbekannte Computer keine drahtlose Verbindung zum WPN824 aufbauen können. MAC-Adressfilterung erschwert den Zugang zu Ihrem Netzwerk, doch die über die drahtlose Verbindung übertragenen Daten sind dabei ungeschützt.
- **Deaktivieren Sie die Ausstrahlung der SSID (Name des drahtlosen Netzwerks).** Wenn Sie die Ausstrahlung der SSID deaktivieren, können nur Geräte mit der richtigen SSID eine Verbindung aufbauen. Dies schützt vor Funktionen zur Entdeckung von drahtlosen Netzwerken (z. B. bei Windows XP), doch die Daten sind immer noch ungeschützt gegen hartnäckige Schnüffler, die spezielle Software wie Wireless Sniffer einsetzen.
- **WEP.** Die Verschlüsselung über Wired Equivalent Privacy (WEP) bietet Sicherheit für Ihre Daten. WEP Shared Key-Authentifizierung und WEP-Datenverschlüsselung stoppen nahezu alle unerwünschten Eindringlinge.
- **WPA-PSK.** Die Verschlüsselung über Wi-Fi Protected Access mit Pre-Shared Key (WPA-PSK) bietet sehr guten Schutz für Ihre Daten. WPA-PSK blockiert alle Eindringlinge. Da dies ein neuer Standard ist, gibt es möglicherweise noch Geräte, die diese Methode nicht unterstützen.
- **Deaktivieren Sie das WLAN.** Wenn Sie das WLAN deaktivieren, können drahtlose Geräte überhaupt nicht mehr mit dem Router kommunizieren. Es empfiehlt sich also, das WLAN auszuschalten, wenn Sie es nicht benutzen und alle Netzwerknutzer Kabelverbindungen verwenden.

Erläuterung der WLAN-Einstellungen

Zur Konfiguration der WLAN-Einstellungen Ihrer Firewall klicken Sie auf den Wireless-Link im Hauptmenü der Browseroberfläche. Damit rufen Sie das hier gezeigte Menü „WLAN-Konfiguration“ auf.

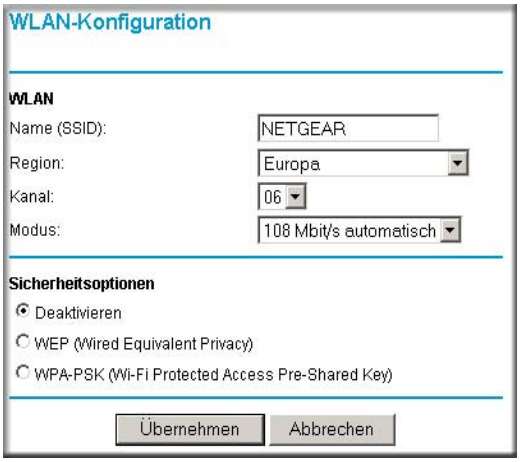


Abbildung 4-3: Das Menü „WLAN-Konfiguration“

- **Name (SSID).** Die SSID wird auch als Netzwerkname bezeichnet. Geben Sie einen Wert aus bis zu 32 alphanumerischen Zeichen für den Netzwerknamen ein. Wenn es an einem Standort mehr als ein WLAN gibt, kann der Datenverkehr über den Netzwerknamen zugeordnet werden. Jedes Gerät, das ein bestimmtes WLAN nutzen soll, muss diese Netzwerk-SSID verwenden. Die Standard-SSID für den WPN824 lautet: **NETGEAR**.
- **Region.** In diesem Feld wird die Region angegeben, in der der WPN824 verwendet werden soll. Möglicherweise kann es gegen das Gesetz verstoßen, die drahtlosen Funktionen Ihres Wireless Routers in einer anderen als der in diesem Feld angegebenen Region zu nutzen.

  Hinweis: Die Funktion zur Auswahl der Region ist möglicherweise nicht in allen Ländern verfügbar.
- **Kanal.** In diesem Feld legen Sie die verwendete Betriebsfrequenz fest. Sofern keine Interferenzen durch andere Access Points in der Umgebung auftreten, brauchen Sie den hier angegebenen Wert nicht zu ändern. Weitere Informationen zu den Funkkanalfrequenzen finden Sie unter „Drahtlose Kanäle“ auf Seite D-7.

- **Modus.** In diesem Feld wird das für die Datenkommunikation verwendete Protokoll festgelegt. Sie können „nur g“, „nur b“ oder „g und b“ auswählen. Bei „nur g“ kommuniziert der WPN824 ausschließlich mit drahtlosen 802.11g-Geräten mit höherer Bandbreite. Bei „nur b“ kommuniziert der WPN824 ausschließlich mit drahtlosen 802.11b-Geräten mit geringerer Bandbreite. Der Modus „g und b“ gewährt Abwärtskompatibilität mit den langsameren drahtlosen 802.11b-Geräten bei gleichzeitiger Nutzung der 802.11g-Kommunikation. Darüber hinaus stehen die Modi „nur 108 MBit/s“ und „108 MBit/s automatisch“ zur Auswahl, mit denen kompatible Wireless-Adapter mit bis zu 108 MBit/s betrieben werden können.
- **Sicherheitsoptionen.** Unter diesem Menüpunkt können Sie die Sicherheitsfunktionen für das WLAN aktivieren. In der folgenden Tabelle sind die grundlegenden WLAN-Sicherheitsoptionen aufgeführt, die Ihnen zur Auswahl stehen. Eine ausführliche Erläuterung der Verschlüsselungsverfahren finden Sie in Anhang D, „Grundlagen drahtloser Netzwerke“.

Tabelle 4-1. Grundlegende WLAN-Sicherheitsoptionen

Feld	Beschreibung
Deaktivieren	Keine Wireless-Sicherheitsfunktionen.
WEP	WEP bietet folgende Optionen: • Open System Mit der offenen Netzwerk-Authentifizierung und 64- oder 128-Bit WEP-Datenverschlüsselung führt der WPN824 64- oder 128-Bit *Datenverschlüsselung* durch, jedoch *keine* Authentifizierung. • Shared Key Beim Authentifizierungsverfahren Shared Key werden die Anmeldung und die Daten verschlüsselt. Legen Sie dazu die Schlüssellänge fest (64- oder 128-Bit Datenverschlüsselung). Geben Sie die Werte für den Schlüssel manuell ein oder geben Sie ein Wort oder eine darstellbare Zeichenfolge in das Feld „Passphrase“ ein. Bei den Zeichen einer Passphrase kommt es auf *Groß- und Kleinschreibung* an, bei manuell eingegebenen Schlüsseln jedoch *nicht*. **Hinweis**: Passphrasen werden nicht von jeder Wireless-Konfigurationssoftware (wie z. B. der Windows-eigenen Wireless-Konfiguration) unterstützt. Geben Sie in diesem Fall den Schlüssel direkt ein. • Automatisch
WPA-PSK	Bei WPA-Pre-Shared Key wird eine *Authentifizierung* durchgeführt, die Daten werden mit 128 Bit verschlüsselt und die Schlüssel dynamisch verändert, wodurch eine Umgehung fast unmöglich gemacht wird. Geben Sie ein Wort oder eine darstellbare Zeichenfolge in das Feld „Passphrase“ ein. Bei diesen Zeichen ist die *Groß- und Kleinschreibung* von Bedeutung. **Hinweis**: WPA wird nicht von allen Wireless-Adapter-Konfigurationen unterstützt. Außerdem ist für den Client-Computer Client-Software erforderlich. In Windows XP mit Service Pack 2 und Windows 2000 mit Service Pack 3 ist die Client-Software mit WPA-Unterstützung enthalten. Trotzdem müssen auch der Wireless-Adapter und der Treiber WPA unterstützen.

Zur Konfiguration der erweiterten WLAN-Einstellungen Ihrer Firewall klicken Sie im Hauptmenü der Browseroberfläche unter „Erweitert“ auf den Link **WLAN-Konfiguration**. Damit rufen Sie das hier gezeigte Menü „Erweiterte WLAN-Einstellungen“ auf:

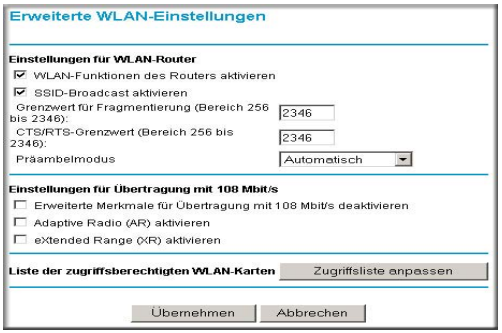


Abbildung 4-4: Das Menü „Erweiterte WLAN-Einstellungen“

- **WLAN-Funktionen des Routers aktivieren.** Wenn Sie den WLAN-Access Point deaktivieren, können drahtlose Geräte nicht auf den WPN824 zugreifen.
- **SSID-Broadcast aktivieren.** Wenn Sie die Ausstrahlung der SSID deaktivieren, können nur Geräte mit der richtigen SSID eine Verbindung aufbauen. Durch Deaktivieren von SSID-Broadcast wird die „Entdeckungsfunktion“ für drahtlose Netzwerke von Produkten wie Windows XP außer Betrieb gesetzt.
- **Liste der zugriffsberechtigten WLAN-Karten.** Wenn die Optionsschaltfläche zum ausschließlichen Zulassen vertrauenswürdiger IP-Adressen aktiviert ist, überprüft der WPN824 die MAC-Adresse der drahtlosen Station und lässt nur Verbindungen zu Computern zu, die auf der Liste der vertrauenswürdigen Computer stehen.

Erforderliche Information vor der Änderung grundlegender WLAN-Einstellungen

Drucken Sie vor der Anpassung Ihrer WLAN-Einstellungen dieses Formular aus und notieren Sie die folgenden Informationen. Wenn Sie mit einem bestehenden drahtlosen Netzwerk arbeiten, erhalten Sie diese Informationen von der Person, die es eingerichtet hat oder dafür verantwortlich ist. Andernfalls wählen Sie die Einstellungen für Ihr drahtloses Netzwerk selbst. Tragen Sie in jedem Fall die Einstellungen für Ihr WLAN an den vorgesehenen Stellen ein.

- **Netzwerkname (SSID)*:*** _____ Durch die SSID wird das drahtlose Netzwerk identifiziert. Sie können bis zu 32 alphanumerische Zeichen dafür verwenden. Bei der SSID wird zwischen *Groß- und Kleinschreibung* unterschieden. Die SSID des Wireless-Adapters muss der SSID des Wireless Routers entsprechen. In manchen Konfigurationsprogrammen (z. B. Windows XP) wird statt SSID die Bezeichnung „Netzwerkname“ verwendet.
- **Wenn WEP-Authentifizierung verwendet wird.** Kreisen Sie eine Option ein: **Open System**, **Shared Key** oder **Automatisch**.

  Hinweis: Wenn Sie **Shared Key** ausgewählt haben, können die anderen Geräte nur mit dem Netzwerk verbunden werden, wenn sie ebenfalls auf **Shared Key** eingestellt und mit dem richtigen Schlüssel konfiguriert sind.

  – **WEP-Schlüsselgröße**. Wählen Sie eine Option: **64 Bit** oder **128 Bit**. Auch hier muss die gleiche Schlüsselgröße für die Wireless-Adapter und den Wireless Router gewählt werden.

  – **WEP-Datenverschlüsselung**. Es gibt zwei Möglichkeiten zur Erstellung von WEP-Datenschlüsseln. Notieren Sie bitte in jedem Fall die Schlüsselwerte an der vorgesehenen Stelle.

    - **Passphrasen-Methode**. _____ Bei diesen Zeichen ist die *Groß- und Kleinschreibung* von Bedeutung. Geben Sie ein Wort oder eine darstellbare Zeichenfolge ein und klicken Sie auf die Schaltfläche zum Erzeugen des Schlüssels. Nicht alle drahtlosen Geräte unterstützen die Passphrasen-Methode.
    - **Manuelle Methode**. Bei diesen Werten spielt die *Groß- und Kleinschreibung keine* Rolle. Geben Sie bei WEP-Verschlüsselung mit 64 Bit eine Hexadezimalzahl mit zehn Stellen ein (Zeichen 0 bis 9 und A bis F in beliebiger Kombination). Geben Sie bei WEP mit 128 Bit eine Hexadezimalzahl mit 26 Stellen ein.

    Schlüssel 1: _____

    Schlüssel 2: _____

    Schlüssel 3: _____

    Schlüssel 4: _____

- **Wenn WPA-PSK-Authentifizierung verwendet wird.**

  – **Passphrase**: _____ Bei diesen Zeichen ist die *Groß- und Kleinschreibung* von Bedeutung. Geben Sie ein Wort oder eine darstellbare Zeichenfolge mit einer Länge von bis zu 63 Zeichen ein. Wenn Sie WPA-PSK verwenden, können die anderen Geräte nur mit dem Netzwerk verbunden werden, wenn sie ebenfalls auf WPA-PSK eingestellt und mit der richtigen Passphrase konfiguriert sind.

Befolgen Sie die in den nachstehenden Abschnitten beschriebenen Verfahren, um den WPN824 zu konfigurieren. Bewahren Sie diese Informationen an einem sicheren Ort auf.

Werkseitige Voreinstellungen

Wenn Sie Ihren WPN824 erwerben, ist er mit den unten stehenden Werkseinstellungen eingerichtet. Diese Einstellungen können Sie mit der Reset-Taste an der Rückseite des Routers wiederherstellen. Befolgen Sie nach der Installation Ihres WPN824 Routers die unten beschriebenen Verfahren, um die Einstellungen an die Anforderungen Ihres Netzwerks anzupassen.

FUNKTION	WERKSEITIGE VOREINSTELLUNG
WLAN-Access Point	**Deaktiviert**
Liste der zugriffsberechtigten WLAN-Karten (MAC-Filterung)	**Alle WLAN-Geräte zugelassen**
SSID-Broadcast	**Aktiviert**
SSID	**NETGEAR**
11b/g-RF-Kanal	**6**
Modus	**108 MBit/s Automatisch**
Authentifizierungsverfahren	**Automatisch**
WEP	**Deaktiviert**
DHCP-Server	**Aktiviert**
DHCP-Bereich	**192.168.1.2 bis 192.168.1.254**

So richten Sie eine erste drahtlose Verbindung ein und testen sie

Hinweis: Wenn Sie einen drahtlosen Computer zum Konfigurieren der WPA-Einstellungen verwenden, wird die Verbindung getrennt, sobald Sie auf „Übernehmen“ klicken. Konfigurieren Sie Ihren Wireless-Adapter neu, damit er den neuen Einstellungen entspricht, oder greifen Sie von einem kabelgebundenen Computer auf den Wireless Router zu, um weitere Änderungen vorzunehmen.

Befolgen Sie die nachstehenden Anweisungen, um eine erste drahtlose Verbindung einzurichten und zu testen. Sobald die erste drahtlose Verbindung hergestellt ist, können Sie die Ihren Anforderungen entsprechenden Sicherheitseinstellungen aktivieren.

1. Melden Sie sich unter der Standard-LAN-Adresse *http://www.routerlogin.net* (oder *http://192.168.1.1*) mit dem Standardbenutzernamen **admin** und dem Standardpasswort **password** bei der WPN824-Firewall an oder verwenden Sie die von Ihnen eingerichtete LAN-Adresse mit dem entsprechenden Passwort.

2. Klicken Sie im Hauptmenü der WPN824-Firewall auf **WLAN-Konfiguration**.

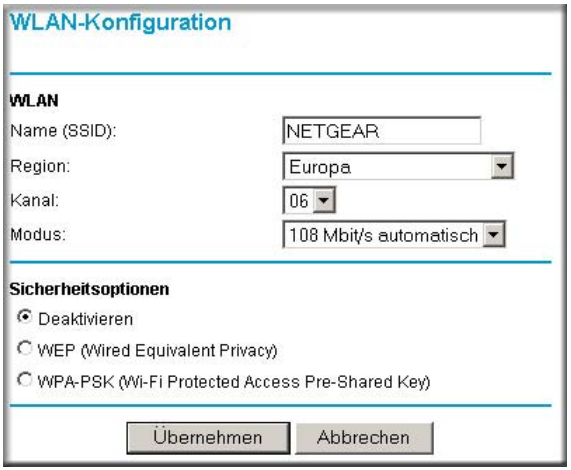


Abbildung 4-5: Das Menü „WLAN-Konfiguration“

3. Wählen Sie einen geeigneten Namen (SSID) für das drahtlose Netzwerk. Geben Sie einen Wert aus bis zu 32 alphanumerischen Zeichen in das Feld „SSID“ ein. Die Standard-SSID lautet: NETGEAR.

   Hinweis: Bei der SSID ist die *Groß- und Kleinschreibung* von Bedeutung; NETGEAR ist daher nicht dasselbe wie nETgear. Außerdem muss die SSID jeglicher Wireless-Adapter der SSID entsprechen, die Sie für den RangeMax Wireless Router WPN824 konfigurieren. Wenn diese Namen nicht übereinstimmen, können die Adapter keine drahtlose Verbindung zum WPN824 herstellen.

4. Legen Sie die Region fest. Wählen Sie die Region, in der das drahtlose Gerät betrieben wird.

5. Legen Sie den Kanal fest. Der Standardkanal ist 6.

   In diesem Feld legen Sie die verwendete Betriebsfrequenz fest. Sofern keine Störungen durch andere drahtlose Router oder Access Points in der Umgebung auftreten, brauchen Sie den hier angegebenen Wert nicht zu ändern. Wählen Sie einen Kanal, der nicht von anderen drahtlosen Netzwerken im Umkreis von ca. 100 Metern Ihrer Firewall verwendet wird. Weitere Informationen zu den Funkkanalfrequenzen finden Sie unter „Drahtlose Kanäle“ auf Seite D-7.

6. Für einen ersten Test sollten Sie die Wireless-Sicherheitsoptionen und die Liste der zugriffsberechtigten WLAN-Karten zunächst deaktiviert lassen.

7. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

	Hinweis: Wenn Sie die Firewall von einem drahtlosen Computer aus konfigurieren und die SSID, den Kanal oder die Sicherheitseinstellungen der Firewall ändern, bricht die drahtlose Verbindung ab, sobald Sie auf „Übernehmen“ klicken. Sie müssen dann die Drahtloseinstellungen Ihres Computers ändern, um sie an die neuen Einstellungen der Firewall anzupassen.

8. Konfigurieren und testen Sie die drahtlose Verbindung Ihrer Computer.

   Konfigurieren Sie den Wireless-Adapter Ihrer Computer so, dass er dieselbe SSID und denselben Kanal wie Ihr Router verwendet. Stellen Sie sicher, dass eine drahtlose Verbindung besteht und dass die Computer über DHCP eine IP-Adresse von der Firewall erhalten können.

   Hinweis: Beim Netzwerknamen (SSID) wird zwischen *Groß- und Kleinschreibung* unterschieden. Wenn NETGEAR der Netzwerkname (SSID) Ihres Wireless Routers ist, müssen Sie unter den Drahtloseinstellungen Ihres Computers NETGEAR angeben (also z. B. nicht „nETgear“).

Sobald die erste drahtlose Verbindung hergestellt ist, können Sie die erweiterten Wireless-Sicherheitsoptionen des Routers konfigurieren.

So konfigurieren Sie WEP

Befolgen Sie zum Konfigurieren der WEP-Datenverschlüsselung die nachstehenden Schritte:

	Hinweis: Wenn Sie einen drahtlosen Computer zum Konfigurieren der WEP-Einstellungen verwenden, wird die Verbindung getrennt, sobald Sie auf „Übernehmen“ klicken. Konfigurieren Sie Ihren Wireless-Adapter in dem Fall entweder neu, damit er den WEP-Einstellungen des Wireless Routers entspricht, oder greifen Sie von einem kabelgebundenen Computer auf den Wireless Router zu, um weitere Änderungen vorzunehmen.

1. Melden Sie sich unter der Standard-LAN-Adresse *http://www.routerlogin.net* mit dem Standardbenutzernamen **admin** und dem Standardpasswort **password** bei der WPN824-Firewall an oder verwenden Sie die von Ihnen eingerichtete LAN-Adresse mit dem entsprechenden Passwort.
2. Klicken Sie im Hauptmenü der WPN824-Firewall auf **WLAN-Konfiguration**.
3. Wählen Sie im Menü „Sicherheitsoptionen“ die Option **WEP**. Damit rufen Sie die WEP-Optionen auf.

4. Wählen Sie aus den Dropdown-Listen das Authentifizierungsverfahren und die Schlüssellänge.

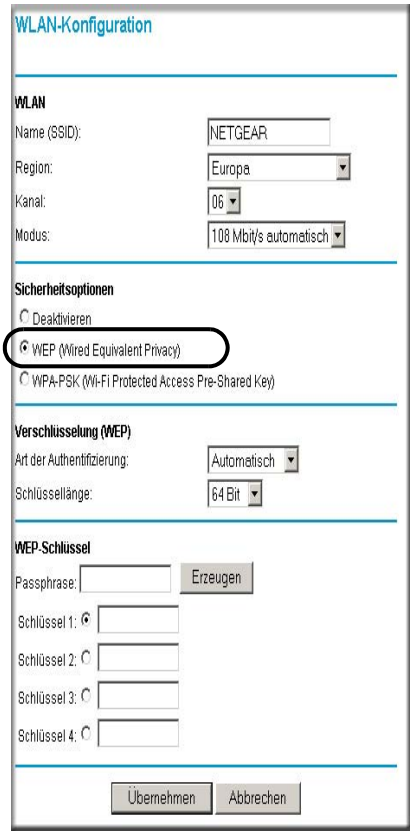


Abbildung 4-6: Das Verschlüsselungsmenü der „WLAN-Konfiguration“

5. Sie können die vier alternativ verwendbaren Schlüssel manuell oder automatisch eingeben. Auf allen Computern und Access Points im WLAN müssen dieselben Werte verwendet werden.
   - Automatisch – Geben Sie ein Wort oder eine darstellbare Zeichenfolge in das Passphrasen-Feld ein und klicken Sie auf die Schaltfläche „Erzeugen“. Bei der Passphrase ist die *Groß- und Kleinschreibung* von Bedeutung; NETGEAR ist daher nicht dasselbe wie nETgear. Die Schlüsselwerte werden automatisch in die vier Schlüsselfelder eingetragen.
   - Manuell – Geben Sie zehn Hexadezimalzeichen ein (Zeichen 0 bis 9 und A bis F bzw. a bis f in beliebiger Kombination). Bei diesen Einträgen spielt die *Groß- und Kleinschreibung keine* Rolle; AA ist dasselbe wie aa.
     Wählen Sie unter den vier Schlüsseln einen beliebigen als „aktiv“ aus.

   Unter „Authentifizierung und WEP-Datenverschlüsselung“ auf Seite D-2 finden Sie eine vollständige Erläuterung all dieser Optionen entsprechend dem Standard IEEE 802.11 für drahtlose Kommunikation.
6. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

So konfigurieren Sie WPA-PSK-Sicherheit im drahtlosen Netzwerk

Hinweis: WPA wird nicht von allen Wireless-Adaptern unterstützt. Außerdem ist Client-Software erforderlich. Windows XP mit Service Pack 2 und Windows 2000 mit Service Pack 3 bieten WPA-Unterstützung. Trotzdem müssen auch der Wireless-Adapter und der Treiber WPA unterstützen. Anweisungen zur Konfiguration von Wireless-Computern oder PDAs für WPA-PSK-Sicherheit finden Sie in der Dokumentation zu dem von Ihnen verwendeten Produkt.

Befolgen Sie zum Konfigurieren von WPA-PSK die nachstehenden Schritte:

1. Klicken Sie im Setup-Bereich des Hauptmenüs auf **WLAN-Konfiguration** und wählen Sie unter „Sicherheitsoptionen“ die Option **WPA-PSK**.

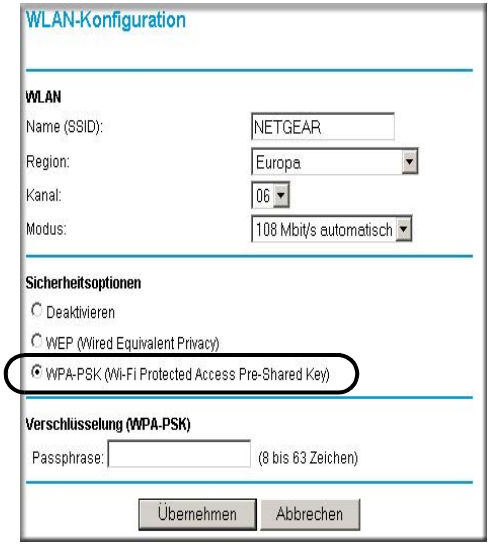


Abbildung 4-7: Das Menü für die WPA-Konfiguration

2. Geben Sie ein Wort oder eine darstellbare Folge von 8–63 Zeichen in das Feld „Passphrase“ ein.
3. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

So schränken Sie den Zugang auf drahtlose Netzwerke über die MAC-Adresse ein

Befolgen Sie die nachstehenden Schritte, um den Zugang anhand der MAC-Adresse einzuschränken:

1. Melden Sie sich unter der Standard-LAN-Adresse *http://www.routerlogin.net* mit dem Standardbenutzernamen **admin** und dem Standardpasswort **password** bei der WPN824-Firewall an oder verwenden Sie die von Ihnen eingerichtete LAN-Adresse mit dem entsprechenden Passwort.

	Hinweis: Wenn Sie die Firewall von einem drahtlosen Computer aus konfigurieren, dessen MAC-Adresse nicht auf der Liste der vertrauenswürdigen IP-Adressen steht, und „Zugriffssteuerung aktivieren“ wählen, bricht die drahtlose Verbindung ab, sobald Sie auf „Übernehmen“ klicken. Greifen Sie in dem Fall entweder von einem kabelgebundenen Computer oder von einem drahtlosen Computer, der auf der Liste steht, auf den Wireless Router zu, um weitere Änderungen vorzunehmen.

2. Klicken Sie im Hauptmenü der WPN824-Firewall unter „Erweitert“ auf **WLAN-Konfiguration**.
3. Klicken Sie im Menü „WLAN-Konfiguration“ auf **Zugriffsliste anpassen**, um das unten gezeigte Menü „Liste der zugriffsberechtigten WLAN-Karten“ aufzurufen:

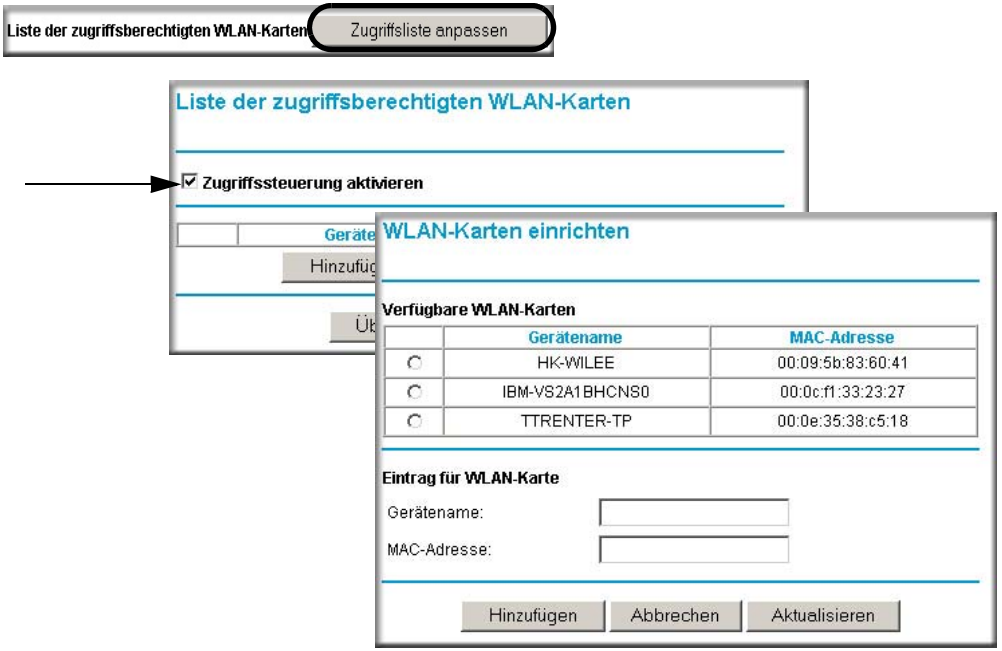


Abbildung 4-8: Einrichtung der Liste der zugriffsberechtigten WLAN-Karten

4. Klicken Sie auf **Hinzufügen**, um ein drahtloses Gerät in die Liste der zugriffsberechtigten WLAN-Karten aufzunehmen. Damit wird die Liste „Verfügbare WLAN-Karten“ aufgerufen.
5. Klicken Sie auf das Kontrollkästchen **Zugriffssteuerung aktivieren**.
6. Wählen Sie dann entweder ein Gerät von der Liste der verfügbaren WLAN-Karten, die der WPN824 in Ihrer Umgebung gefunden hat, oder geben Sie die MAC-Adresse und den Gerätenamen des Geräts ein, das Sie verwenden möchten. Die MAC-Adresse ist normalerweise auf den Wireless-Adapter aufgedruckt.

   Hinweis: Sie können MAC-Adressen aus dem Menü „Angeschlossene Geräte“ der Firewall in das MAC-Adressfeld in diesem Menü kopieren. Konfigurieren Sie dazu jeden drahtlosen Computer so, dass er eine drahtlose Verbindung zur Firewall herstellt. Der Computer sollte daraufhin im Menü „Angeschlossene Geräte“ aufgeführt werden.
7. Klicken Sie auf **Hinzufügen**, um dieses drahtlose Gerät in die Liste der zugriffsberechtigten WLAN-Karten aufzunehmen. Der Bildschirm wechselt nun wieder zum Listenbildschirm. Wiederholen Sie diese Schritte für jedes weitere Gerät, das Sie in die Liste aufnehmen möchten.
8. Klicken Sie unbedingt auf **Übernehmen**, um die Einstellungen Ihrer Liste für die drahtlose Zugriffssteuerung zu speichern.

Jetzt können nur Geräte, die in dieser Liste aufgeführt sind, eine drahtlose Verbindung zum WPN824 aufnehmen.

Kapitel 5
Content-Filterung

In diesem Kapitel erfahren Sie, wie Sie Ihr Netzwerk durch die Content-Filterung des RangeMax Wireless Router WPN824 schützen können. Diese Funktionen finden Sie unter der Überschrift **Content-Filterung** im Hauptmenü der Browseroberfläche.

Überblick über die Content-Filterung

Der RangeMax Wireless Router WPN824 bietet Ihnen Optionen für die Content-Filterung im Internet sowie zur Protokollierung von Browsing-Vorgängen und sofortige Warnmeldungen per E-Mail. Eltern und Netzwerkadministratoren können den Zugriff nach Uhrzeit, Website-Adressen und Stichwörtern für Website-Adressen einschränken. Außerdem können Sie den Internetzugriff auf Anwendungen oder Dienste sperren, z. B. für Chat oder Online-Spiele.

Klicken Sie zur Konfiguration dieser Router-Funktionen auf die Optionen unter der Überschrift **Content-Filterung** im Hauptmenü der Browseroberfläche. Diese Optionen werden im Folgenden beschrieben:

Sperren des Zugriffs auf Internet-Websites

Über den WPN824 Router können Sie den Internetzugriff nach Website-Adressen und Stichwörtern für Website-Adressen sperren. Die Stichwortliste kann bis zu 255 Einträge umfassen. Das Menü „Sites sperren“ wird in Abbildung 5-1 gezeigt:

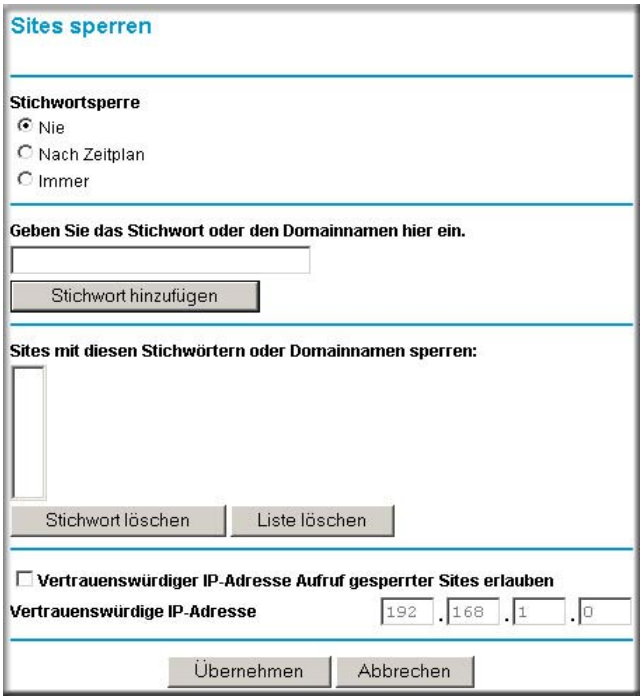


Abbildung 5-1: Das Menü „Sites sperren“

Wählen Sie zur Aktivierung der **Stichwortsperre** entweder **Nach Zeitplan** oder **Immer** und klicken Sie dann auf **Übernehmen**. Wenn Sie die Sperre nach Zeitplan vornehmen möchten, muss im Menü „Zeitplan“ ein Uhrzeitbereich angegeben sein.

Geben Sie Stichwörter oder Domainnamen, die Sie hinzufügen möchten, in das entsprechende Feld ein und klicken Sie auf **Stichwort hinzufügen** und dann auf **Übernehmen**.

Markieren Sie Stichwörter oder Domainnamen, die Sie löschen möchten, in der Liste und klicken Sie auf **Stichwort löschen** und dann auf **Übernehmen**.

Beispiele für die Anwendung von Stichwörtern:

- Wenn das Stichwort „XXX“ angegeben ist, wird die URL <http://www.schlimmesachen.de/xxx.html> gesperrt.

- Ist das Stichwort „.com“ angegeben, können nur Websites mit anderen Domainerweiterungen (wie .de oder .net) aufgerufen werden.
- Wenn Sie zu bestimmten Zeiten jeglichen Zugriff auf das Internet sperren möchten, geben Sie als Stichwort „.“ ein und legen Sie im Menü „Zeitplan“ die Uhrzeiten fest.

Um einen vertrauenswürdigen Benutzer festzulegen, geben Sie die IP-Adresse des entsprechenden PCs unter **Vertrauenswürdige IP-Adresse** ein und klicken Sie auf **Übernehmen**.

Sie können eine vertrauenswürdige IP-Adresse angeben, die von den Sperren und Protokollen ausgenommen ist. Da die Identifikation per IP-Adresse erfolgt, sollten Sie den vertrauenswürdigen PC mit einer festen IP-Adresse versehen.

Sperren des Zugriffs auf Internetdienste

Über den WPN824 Router können Sie die Nutzung bestimmter Internetdienste durch PCs in Ihrem Netzwerk sperren. Diese Funktion wird als Dienstesperre oder Portfilterung bezeichnet. Das Menü „Dienste sperren“ wird hier gezeigt:

Abbildung 5-2: Das Menü „Dienste sperren“

Dienste sind Funktionen, die auf Anfrage von Client-Computern durch Server-Computer ausgeführt werden. Webserver liefern z. B. Webseiten, Zeitserver liefern Informationen zu Datum und Uhrzeit und Spiele-Hosts liefern Daten über die Züge anderer Spieler. Wenn ein Computer in Ihrem Netzwerk eine Dienstanfrage an einen Server im Internet richtet, ist der entsprechende Dienst durch eine Portnummer gekennzeichnet. Diese Nummer erscheint als Zielportnummer in den übertragenen IP-Paketen. Ein Paket, das mit der Zielportnummer 80 gesendet wird, ist beispielsweise eine HTTP-Anfrage (an den Webserver).

Wählen Sie zur Aktivierung von **Dienste sperren** entweder **Nach Zeitplan** oder **Immer** und klicken Sie dann auf **Übernehmen**. Wenn Sie die Sperre nach Zeitplan vornehmen möchten, muss im Menü „Zeitplan“ ein Uhrzeitbereich angegeben sein.

Klicken Sie zur Angabe eines Dienstes, der gesperrt werden soll, auf **Hinzufügen**. Damit rufen Sie das hier gezeigte Menü „Dienstsperren einrichten“ auf:

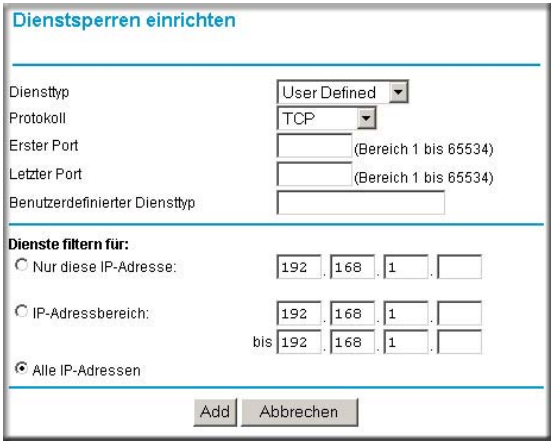


Abbildung 5-3: Das Menü „Dienstsperren einrichten“

Wählen Sie in der Liste **Diensttyp** die Anwendung bzw. den Dienst, der zugelassen oder gesperrt werden soll. Die Liste enthält bereits mehrere gängige Dienste, Ihre Wahl ist dadurch jedoch nicht eingeschränkt. Wenn Sie zusätzliche Dienste oder Anwendungen hinzufügen möchten, wählen Sie **Benutzerdefinierter Diensttyp**.

Einrichten eines benutzerdefinierten Dienstes

Zum Definieren von Diensten benötigen Sie zunächst die Portnummer oder den Portnummernbereich der Anwendung. Die Portnummern für viele gebräuchliche Protokolle werden von der Internet Engineering Task Force (IETF) definiert und in RFC1700, „Assigned Numbers“ (Zugewiesene Nummern), veröffentlicht. Portnummern für andere Anwendungen werden gewöhnlich von den Herausgebern der Anwendung im Bereich 1024 bis 65535 gewählt. Sie erhalten diese Informationen normalerweise durch Nachfrage beim Herausgeber oder bei Benutzer- und Newsgruppen.

Geben Sie die Nummern für **Erster Port** und **Letzter Port** ein. Wenn die Anwendung nur eine Portnummer verwendet, geben Sie diese in beide Felder ein.

Wenn Sie wissen, ob die Anwendung TCP oder UDP nutzt, wählen Sie das entsprechende Protokoll. Wenn Sie nicht sicher sind, wählen Sie **TCP/UDP**.

Sperren von Diensten für bestimmte IP-Adressen

Unter „Dienste filtern für“ können Sie den angegebenen Dienst für einen einzelnen Computer, eine Reihe von Computern (mit aufeinander folgenden IP-Adressen) oder alle Computer in Ihrem Netzwerk sperren.

Sperrungen zu bestimmten Zeiten

Mit dem WPN824 Router können Sie angeben, wann die Sperrung angewendet werden soll. Das Menü „Zeitplan“ wird hier gezeigt:

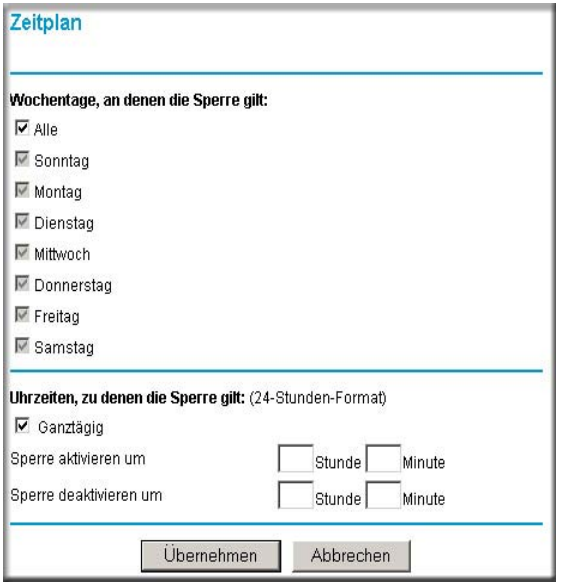


Abbildung 5-4: Das Menü „Zeitplan“

- Anhand dieses Zeitplans können Sie Inhalte sperren. Aktivieren Sie diese Option, wenn Sie einen Zeitplan für die Content-Filterung einrichten möchten. Klicken Sie auf **Übernehmen**.
- **Wochentage, an denen die Sperre gilt**: Wählen Sie die gewünschten Tage aus, indem Sie die entsprechenden Kästchen aktivieren. Wählen Sie **Alle**, um alle Wochentage zu aktivieren. Klicken Sie auf **Übernehmen**.
- **Uhrzeiten, zu denen die Sperre gilt**: Legen Sie die Zeiten, zu denen die Sperre aktiviert und deaktiviert werden soll, im 24-Stunden-Format fest. Wählen Sie **Ganztägig**, damit die Sperre rund um die Uhr wirksam wird. Klicken Sie auf **Übernehmen**.

Wählen Sie unbedingt im E-Mail-Menü die richtige Zeitzone.

Ansehen von Protokollen für Internetzugriff oder versuchten Zugriff

Das Protokoll ist eine detaillierte Auflistung aller Websites, auf die Sie zugegriffen haben oder dies versucht haben. Das Protokoll kann bis zu 128 Einträge umfassen. Protokolleinträge werden nur angezeigt, wenn die Stichwortsperre aktiviert ist. Für Benutzer, die als vertrauenswürdig eingestuft sind, werden keine Protokolleinträge vorgenommen. Hier sehen Sie ein Beispiel:

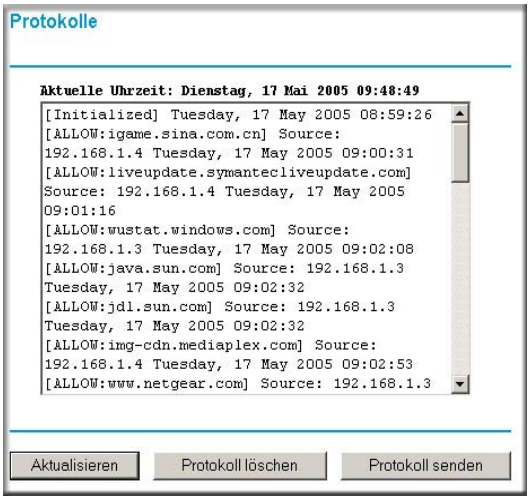


Abbildung 5-5: Das Menü „Protokolle“

Tabelle 5-1 enthält eine Beschreibung der Protokolleinträge.

Tabelle 5-1. Beschreibung der Protokolleinträge

Feld	Beschreibung
Nummer	Die laufende Nummer der Protokolleinträge zur Content-Filterung. 128 Einträge von Nummer 0 bis 127 sind möglich. Im Protokoll erscheinen jeweils die 128 letzten Einträge.
Datum und Uhrzeit	Datum und Uhrzeit der Aufzeichnung des Protokolleintrags.
IP-Adresse	Die IP-Adresse des Ausgangsgeräts für diesen Protokolleintrag.
Vorgang	Hier ist zu sehen, ob der Zugriff zugelassen oder gesperrt wurde.
URL	Der Name oder die IP-Adresse der Website oder Newsgruppe, die besucht bzw. auf die der Zugriff versucht wurde.

Tabelle 5-2 enthält eine Beschreibung der Schaltflächen zur Bearbeitung der Protokolle.

Tabelle 5-2. Schaltflächen zur Bearbeitung der Protokolle

Feld	Beschreibung
Aktualisieren	Klicken Sie auf diese Schaltfläche, um den Protokollbildschirm zu aktualisieren.
Protokoll löschen	Klicken Sie auf diese Schaltfläche, um die Protokolleinträge zu löschen.
Protokoll senden	Klicken Sie auf diese Schaltfläche, um das Protokoll umgehend per E-Mail zu senden.

Einrichten von Benachrichtigungen und Zugriffswarnungen per E-Mail

Um Protokolle und Benachrichtigungen per E-Mail zu erhalten, müssen Sie Ihre E-Mail-Angaben in das hier abgebildete E-Mail-Menü eintragen:

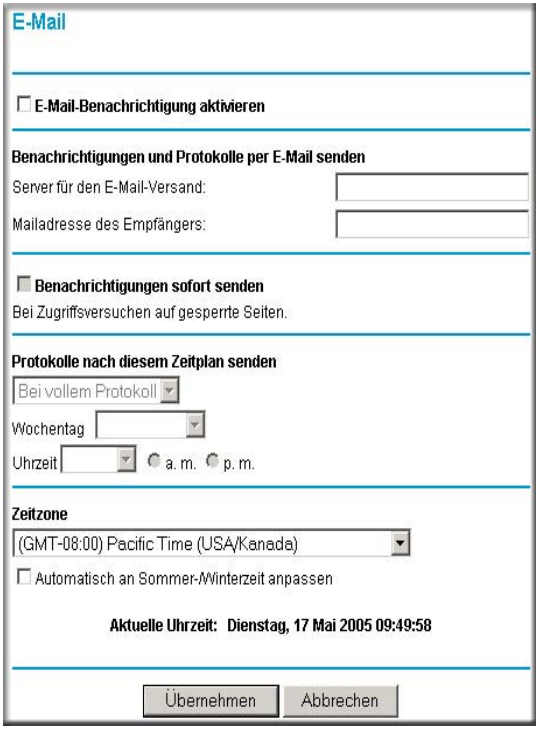


Abbildung 5-6: Das Menü „E-Mail“

- **E-Mail-Benachrichtigung aktivieren**
  Aktivieren Sie dieses Kästchen, wenn Sie vom Router Protokolle und Benachrichtigungen per E-Mail erhalten möchten.
- **Server für den E-Mail-Versand**
  Geben Sie den Namen des SMTP-Servers Ihres ISP (für den Versand von E-Mail) ein (z. B. mail.meinISP.de). Möglicherweise finden Sie diese Informationen im Konfigurationsmenü Ihres E-Mail-Programms. Wenn Sie dieses Feld leer lassen, werden keine Protokolle und Benachrichtigungen per E-Mail gesendet.
- **Mailadresse des Empfängers**
  Geben Sie die E-Mail-Adresse ein, an die Protokolle und Benachrichtigungen gesendet werden sollen. Diese E-Mail-Adresse wird gleichzeitig als die des Absenders verwendet. Wenn Sie dieses Feld leer lassen, werden keine Protokolle und Benachrichtigungen per E-Mail gesendet.

Mit den folgenden Optionen können Sie Protokolle automatisch an die angegebene E-Mail-Adresse senden lassen:

- **Benachrichtigungen sofort senden**
  Aktivieren Sie dieses Kästchen, wenn Sie immer sofort über den versuchten Zugriff auf eine gesperrte Website benachrichtigt werden möchten.
- **Protokolle nach diesem Zeitplan senden**
  Damit geben Sie an, wie oft die Protokolle gesendet werden sollen: **Stündlich**, **Täglich**, **Wöchentlich** oder **Bei vollem Protokoll**.
  - Wochentag für die Protokollsendung
    Hier wird angegeben, an welchem Wochentag das Protokoll gesendet werden soll. Der Eintrag ist erforderlich, wenn das Protokoll wöchentlich gesendet werden soll.
  - Uhrzeit für die Protokollsendung
    Hier wird angegeben, zu welcher Uhrzeit das Protokoll gesendet werden soll. Der Eintrag ist erforderlich, wenn das Protokoll täglich oder wöchentlich gesendet werden soll.

  Wenn die Option für wöchentliche, tägliche oder stündliche Benachrichtigung gewählt wurde und das Protokoll vor Ablauf der angegebenen Zeit voll ist, wird es automatisch an die angegebene E-Mail-Adresse gesendet. Nach dem Senden des Protokolls wird dieses automatisch aus dem Speicher des Routers gelöscht. Wenn der Router die Protokolldatei nicht per E-Mail senden kann, wird der Protokoll-Zwischenspeicher möglicherweise zu voll. In diesem Fall überschreibt der Router das Protokoll und löscht seinen Inhalt.

Der WPN824 Router nutzt das NTP-Protokoll (Network Time Protocol) zum Abruf der aktuellen Uhrzeit und des Datums von einem der NTP-Server im Internet. Zur Lokalisierung der Uhrzeit für Ihre Protokolleinträge müssen Sie Ihre Zeitzone angeben:

- **Zeitzone**
  Wählen Sie die Zeitzone für Ihren Standort. Diese Einstellung wird für den Sperren-Zeitplan und zur zeitlichen Bestimmung der Protokolleinträge verwendet.
- **Automatisch an Sommer-/Winterzeit anpassen**
  Aktivieren Sie dieses Kästchen, wenn für Ihre Zeitzone eine Sommerzeit verwendet wird.

Kapitel 6
Wartung

In diesem Kapitel erfahren Sie, wie Sie die Wartungsfunktionen Ihres RangeMax Wireless Router WPN824 verwenden. Diese Funktionen finden Sie unter der Überschrift **Wartung** im Hauptmenü der Browseroberfläche.

Anzeigen der Statusinformationen des Wireless Routers

Das Menü „Routerstatus“ enthält Informationen zum Status und zur Auslastung. Klicken Sie zum Aufrufen des Bildschirms „Routerstatus“ im Menü der Konfigurationsoberfläche unter „Wartung“ auf den Menüpunkt **Routerstatus**.

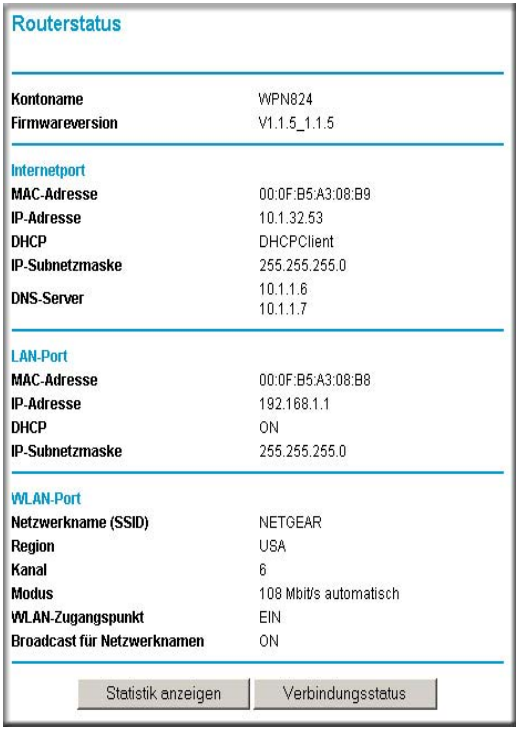


Abbildung 6-1: Der Bildschirm „Routerstatus“

Dieser Bildschirm listet die folgenden Parameter auf:

Tabelle 6-1. Wireless Router – Statusfelder

Feld	Beschreibung
Kontoname	Dieses Feld zeigt den Hostnamen an, der dem Router zugewiesen wurde.
Firmwareversion	Diese Feld zeigt die Firmwareversion des Routers an.
Internetport	Diese Parameter beziehen sich auf den Internet-WAN-Port des Routers.
MAC-Adresse	Dieses Feld zeigt die MAC-Adresse (Media Access Control) an, die vom Internet-WAN-Port des Routers verwendet wird.
IP-Adresse	Dieses Feld zeigt die IP-Adresse an, die vom Internet-WAN-Port des Routers verwendet wird. Wenn keine IP-Adresse angezeigt wird, kann der Router keine Verbindung zum Internet herstellen.
DHCP	Wenn hier „Kein Eintrag“ eingestellt ist, ist der Router so konfiguriert, dass er eine feste IP-Adresse im WAN verwendet. Ist dagegen „DHCP Client“ eingestellt, ist der Router so konfiguriert, dass er seine IP-Adresse dynamisch vom Internetdienstanbieter bezieht.
IP-Subnetzmaske	Dieses Feld zeigt die IP-Subnetzmaske an, die vom Internet-WAN-Port des Routers verwendet wird.
DNS-Server	In diesem Feld erscheinen die DNS-Adressen, die der Router verwendet.
LAN-Port	Diese Parameter beziehen sich auf den LAN-Port des Routers.
MAC-Adresse	Dieses Feld zeigt die MAC-Adresse (Media Access Control) an, die LAN-seitig verwendet wird.
IP-Adresse	Dieses Feld zeigt die IP-Adresse an, die LAN-seitig verwendet wird. Die Standardeinstellung ist „192.168.1.1“.
IP-Subnetzmaske	Dieses Feld zeigt die IP-Subnetzmaske an, die LAN-seitig verwendet wird. Die Standardeinstellung ist „255.255.255.0“.
DHCP	Zeigt an, ob der im Router integrierte DHCP-Server für die über das LAN angeschlossenen Geräte aktiviert ist.

Tabelle 6-1. Wireless Router – Statusfelder

Feld	Beschreibung
WLAN-Port	Diese Parameter beziehen sich auf den Access Point des Routers.
MAC-Adresse	Dieses Feld zeigt die MAC-Adresse (Media Access Control) an, die vom Access Point des Routers verwendet wird.
Netzwerkname (SSID)	Dieses Feld zeigt den Netzwerknamen (SSID) an, der vom Access Point des Routers verwendet wird. Die Standardeinstellung ist „NETGEAR“.
Region	Dieses Feld zeigt die geografische Region an, in der der Router eingesetzt wird. In manchen Ländern ist die Verwendung der drahtlosen Eigenschaften des Routers möglicherweise gesetzlich verboten.
Kanal	Gibt den verwendeten Kanal des Access Points an. Die Frequenzen der einzelnen Kanäle finden Sie unter „Drahtlose Kanäle“ auf Seite D-7.

Klicken Sie auf die Schaltfläche **Verbindungsstatus**, um den Verbindungsstatus anzuzeigen (vgl. Abb. unten).

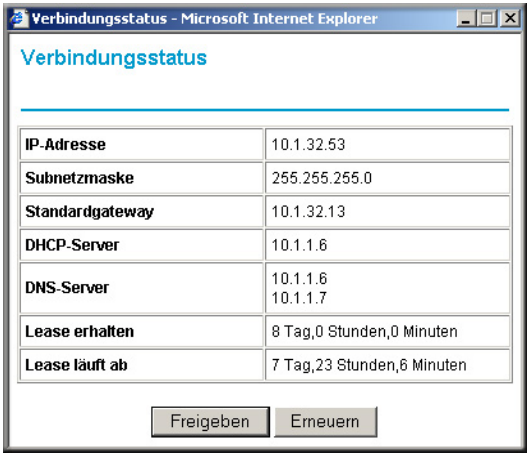


Abbildung 6-2: Der Bildschirm „Verbindungsstatus“

Dieser Bildschirm enthält die folgenden Angaben:

Tabelle 6-2: Angaben zum Verbindungsstatus

Feld	Beschreibung
IP-Adresse	Die dem Router zugewiesene WAN-(Internet)-IP-Adresse.
Subnetzmaske	Die dem Router zugewiesene WAN-(Internet)-Subnetzmaske.

Tabelle 6-2: Angaben zum Verbindungsstatus

Feld	Beschreibung
Standardgateway	Das WAN-(Internet)-Standardgateway, mit dem der Router kommuniziert.
DHCP-Server	Die IP-Adresse des DHCP-Servers, der die Adressen für die IP-Konfiguration bereitgestellt hat.
DNS-Server	Die IP-Adresse des DNS-Servers, der den Netzwerknamen für die IP-Adressenumwandlung bereitstellt.
Lease erhalten	Verstrichene Zeit seit Erhalt des DHCP-Lease.
Lease läuft ab	Verbleibende Zeit bis zum Ablauf des DHCP-Lease.
Freigeben	Durch Klicken auf die Schaltfläche **Freigeben** wird das DHCP-Lease freigegeben.
Erneuern	Durch Klicken auf die Schaltfläche **Erneuern** wird das DHCP-Lease erneuert.

Wenn Sie auf die Schaltfläche **Statistik anzeigen** klicken, wird die unten abgebildete Statistik zur Auslastung des Routers angezeigt.

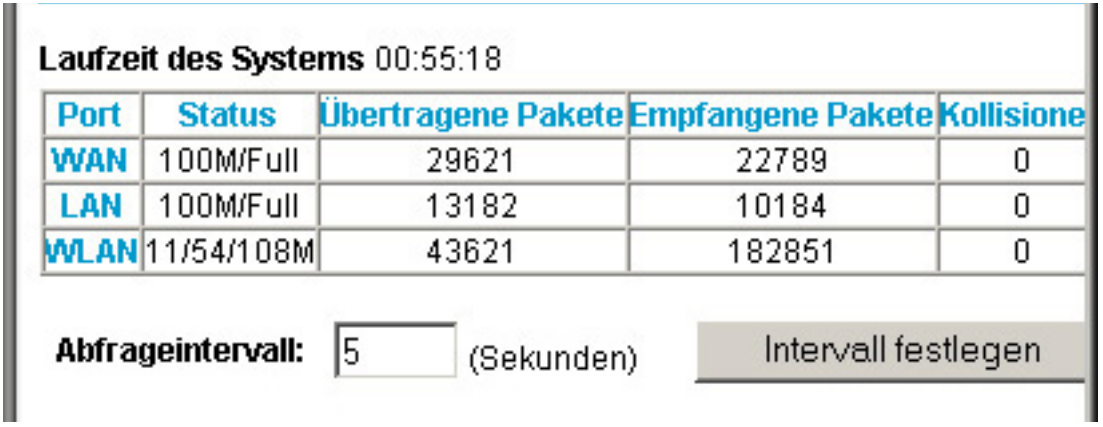


Abbildung 6-3: Der Bildschirm „Routerstatistik“

Dieser Bildschirm enthält die folgenden statistischen Angaben:

Tabelle 6-3: Angaben zur Routerstatistik

Feld	Beschreibung
Port	Die statistischen Angaben für den WAN (Internet)-Port, den LAN (lokalen)-Port und das WLAN. Für jeden der Ports zeigt dieser Bildschirm die folgenden Angaben an:
Status	Der Verbindungsstatus.
Übertragene Pakete	Die Anzahl der Pakete, die seit dem letzten Zurücksetzen oder manuellen Löschen über diesen Port übertragen wurden.

Tabelle 6-3: Angaben zur Routerstatistik

Feld	Beschreibung
Empfangene Pakete	Die Anzahl der Pakete, die seit dem letzten Zurücksetzen oder manuellen Löschen über diesen Port empfangen wurden.
Kollisionen	Die Anzahl der Kollisionen auf diesem Port seit dem letzten Zurücksetzen oder manuellen Löschen.
Übertragene Bytes pro Sekunde	Die aktuelle Übertragungsbandbreite (ausgehende Bandbreite).
Empfangene Bytes pro Sekunde	Die aktuelle Empfangsbandbreite (ankommende Bandbreite).
Laufzeit	Die verstrichene Zeit seit dem letzten Neustart des Routers.
Abfrageintervall	Gibt an, in welchem Zeitabstand die Statistiken in diesem Fenster aktualisiert werden. Wenn Sie auf **Anhalten** klicken, wird die Anzeige angehalten.
Intervall festlegen	Geben Sie eine Zeit ein und klicken Sie auf diese Schaltfläche, um den Abstand zwischen den Abfragen festzulegen.
Anhalten	Klicken Sie auf die Schaltfläche **Anhalten**, um die Abfrageinformationen anzuhalten.

Anzeigen der angeschlossenen Geräte

Das Menü „Angeschlossene Geräte“ enthält eine Tabelle aller IP-Geräte, die der Router im lokalen Netzwerk gefunden hat (vgl. Abbildung unten). Klicken Sie zum Aufrufen der Tabelle im Hauptmenü der Browseroberfläche unter „Wartung“ auf **Angeschlossene Geräte**.

Abbildung 6-4: Das Menü „Angeschlossene Geräte“

Die Tabelle zeigt zu jedem Gerät die IP-Adresse, den NetBIOS-Hostnamen (falls verfügbar) und die MAC-Adresse an. Bitte beachten Sie, dass die Tabellendaten beim Booten des Routers verloren gehen und erst wieder verfügbar sind, wenn der Router die Geräte gefunden hat. Klicken Sie auf die Schaltfläche **Aktualisieren**, um den Router zu zwingen, nach neuen Geräten zu suchen.

Verwaltung der Konfigurationsdateien

Die Konfigurationseinstellungen des WPN824 Routers sind in einer Konfigurationsdatei auf dem Router gespeichert. Diese Datei kann zur Sicherung auf dem PC eines Benutzers gespeichert, vom PC abgerufen (wiederhergestellt) oder auf die Werkseinstellungen zurückgesetzt werden.

Wählen Sie im Hauptmenü unter „Wartung“ die Option **Einstellungen sichern**, um das unten abgebildete Menü aufzurufen.

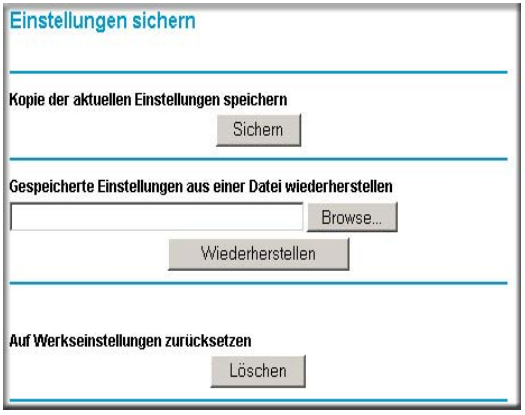


Abbildung 6-5: Das Menü „Einstellungen sichern“

Die drei in diesem Menü verfügbaren Optionen werden in den folgenden Abschnitten erläutert.

Wiederherstellung und Sichern der Konfiguration

Mit Hilfe der Optionen **Wiederherstellen** und **Sichern** im Menü „Einstellungen sichern“ können Sie eine Datei mit den Konfigurationseinstellungen Ihres Routers abspeichern und aufrufen.

Klicken Sie zum Speichern der Einstellungen auf die Schaltfläche **Sichern**. Ihr Browser extrahiert die Konfigurationsdatei vom Router und fordert Sie auf, einen Speicherort für die Datei anzugeben. An dieser Stelle können Sie der Datei auch einen aussagekräftigen Namen wie pacbell.cfg geben.

Zum Wiederherstellen der Einstellungen mit Hilfe einer auf einem PC gespeicherten Konfigurationsdatei geben Sie den vollständigen Pfad zu dieser Datei ein oder klicken Sie auf die Schaltfläche **Durchsuchen**, um danach zu suchen. Wenn Sie die Datei gefunden haben, klicken Sie auf die Schaltfläche **Wiederherstellen**, um die Datei an den Router zu senden. Der Router wird dann automatisch neu gestartet.

Warnung: Unterbrechen Sie den Neustartvorgang unter keinen Umständen.

Löschen der Konfiguration

Manchmal ist es sinnvoll, die ursprünglichen Einstellungen des Routers wiederherzustellen. Die Funktion **Löschen** setzt den Router wieder in den Auslieferungszustand zurück. Nach dem Löschen sämtlicher Einstellungen lautet der Benutzername für den Router „admin“, das Passwort „password“ und die LAN-IP-Adresse „192.168.1.1“. Beim Löschen wird zudem automatisch der DHCP-Server des Routers aktiviert.

Klicken Sie zum Löschen der Konfiguration auf die Schaltfläche **Löschen**.

Wenn Sie die Werkseinstellungen wiederherstellen möchten, ohne das Anmeldekennwort oder die IP-Adresse zu kennen, müssen Sie die Reset-Taste an der Rückseite des Routers betätigen. Nähere Informationen dazu finden Sie unter „Wiederherstellen von Werkseinstellungen und Passwort“ auf Seite 7-7.

Aktualisieren der Routersoftware

Tipp: Um sicherzustellen, dass Sie immer die neueste Firmwareversion verwenden, sollten Sie den **Assistenten für die Aktualisierung der Firmware** aktivieren. So entdeckt der Router neue Firmwareversionen automatisch im Internet und weist Sie darauf hin.

Dieser Bildschirm wird bei der Anmeldung angezeigt, solange Sie nicht die Option **Diese Meldung nicht mehr anzeigen** angeklickt haben.

Hinweis: Bevor Sie die Routersoftware aktualisieren, sollten Sie Ihre Konfigurationseinstellungen mit der Sicherungsfunktion des Routers sichern. Bei jeder Softwareaktualisierung werden die Routereinstellungen auf die Werkseinstellungen zurückgesetzt. Nach Abschluss der Aktualisierung können Sie Ihre Einstellungen mit Hilfe der gesicherten Datei wiederherstellen.

Die Software des WPN824 Routers ist in einem Flash-Speicher gespeichert und kann aktualisiert werden, wenn NETGEAR neue Software herausbringt. Aktualisierungsdateien können von der NETGEAR-Website heruntergeladen werden. Wenn die Aktualisierungsdatei komprimiert ist (Dateierweiterung „ZIP“), müssen Sie die Datei extrahieren, bevor Sie sie an den Router senden. Die Aktualisierungsdatei kann über einen Browser an den Router gesendet werden.

Hinweis: Zum Hochladen neuer Firmware auf den WPN824 Router benötigen Sie einen Browser, der HTTP-Uploads unterstützt. NETGEAR empfiehlt die Verwendung von Microsoft Internet Explorer oder Netscape Navigator Version 3.0 oder höher.

Wählen Sie im Hauptmenü unter „Wartung“ die Option **Router aktualisieren**, um das unten abgebildete Menü aufzurufen.

Abbildung 6-6: Das Menü „Router aktualisieren“

So laden Sie neue Firmware hoch:

1. Laden Sie die neue Software von der Website von NETGEAR herunter und entzippen Sie die Datei (falls es sich um eine ZIP-Datei handelt).
2. Klicken Sie im Menü „Router aktualisieren“ auf die Schaltfläche **Durchsuchen** und wählen Sie den Speicherort der Aktualisierungsdatei aus.
3. Klicken Sie auf **Hochladen**.

   Hinweis: Achten Sie beim Hochladen der Software auf den WPN824 Router darauf, den Vorgang nicht zu unterbrechen (z. B. durch Schließen des Browserfensters, Klicken auf einen Link oder Laden einer neuen Seite). Wenn der Ladevorgang unterbrochen wird, kann dies Ihren Router zerstören. Nach Abschluss des Hochladevorgangs wird der Router automatisch neu gestartet. Der Aktualisierungsvorgang dauert in der Regel ungefähr eine Minute.

Im Anschluss an die Aktualisierung der Firmware muss der Router unter Umständen neu konfiguriert werden.

Ändern des Administratorpassworts

	Hinweis: Bevor Sie das Routerpasswort ändern, sollten Sie Ihre Konfigurationseinstellungen mit der Sicherungsfunktion des Routers sichern. Wenn Sie das neue Passwort nach dem Ändern vergessen, müssen Sie den Router auf die Werkseinstellungen zurücksetzen, um sich mit dem voreingestellten Passwort „password“ anmelden zu können. In diesem Fall müssen Sie jedoch sämtliche Konfigurationseinstellungen des Routers wiederherstellen. Wenn Sie Ihren Router auf die Werkseinstellungen zurücksetzen müssen, können Sie Ihre Einstellungen mit Hilfe der Sicherungsdatei wiederherstellen.

Das voreingestellte Passwort für die Konfigurationsoberfläche des Routers lautet „password“. NETGEAR empfiehlt, dieses Passwort zu einem sichereren Passwort zu ändern.

Wählen Sie im Hauptmenü unter „Wartung“ die Option **Passwort festlegen**, um das unten abgebildete Menü aufzurufen.

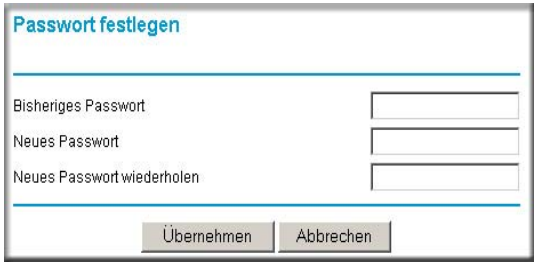


Abbildung 6-7: Das Menü „Passwort festlegen“

Geben Sie zum Ändern des Passworts zuerst das alte Passwort und dann zweimal das neue Passwort ein. Klicken Sie auf **Übernehmen**.

Kapitel 7
Fehlerbehebung

In diesem Kapitel finden Sie Hinweise zur Behebung von Fehlern bei Ihrem RangeMax Wireless Router WPN824. Nach der Beschreibung eines Problems finden Sie jeweils eine Anleitung zur Diagnose und Behebung des Problems.

Basisbetrieb

Nach dem Einschalten des Routers sollten die folgenden Ereignisse in der angegebenen Reihenfolge auftreten:

1. Überprüfen Sie nach dem Einschalten, ob die Stromanzeige leuchtet.
2. Überprüfen Sie nach ungefähr 10 Sekunden die folgenden Punkte:
   a. Die Stromanzeige sollte grün leuchten.
   b. Die LAN-Port-Anzeigen aller lokalen Ports, zu denen eine Verbindung besteht, sollten leuchten.
   c. Die Internet-Portanzeige sollte leuchten.

   Wenn die Anzeige eines Ports leuchtet, wurde eine Verbindung zum angeschlossenen Gerät hergestellt. Wenn an einen LAN-Port ein100-MBit/s-Gerät angeschlossen ist, vergewissern Sie sich, dass die Anzeige dieses Ports grün leuchtet. Wenn der Port mit 10 MBit/s kommuniziert, leuchtet die Anzeige gelb.

Wenn eine dieser Bedingungen nicht erfüllt ist, gehen Sie zum entsprechenden Abschnitt.

Stromanzeige leuchtet nicht

Wenn die Stromanzeige oder andere Anzeigen beim Einschalten des Routers nicht aufleuchten, sollten Sie die folgenden Schritte durchführen:

- Vergewissern Sie sich, dass das Netzkabel ordnungsgemäß mit dem Router verbunden ist und dass das Netzteil ordnungsgemäß an eine funktionierende Steckdose angeschlossen ist.
- Vergewissern Sie sich, dass Sie das von NETGEAR für dieses Produkt mitgelieferte Netzteil (12 V/1 A Gleichstrom) verwenden.

Wenn der Fehler sich dadurch nicht beheben lässt, liegt ein Hardwarefehler vor. Wenden Sie sich an den technischen Support.

Anzeigen erlöschen nicht

Beim Einschalten des Routers leuchten die Anzeigen für ungefähr 10 Sekunden auf und erlöschen dann wieder. Wenn alle Anzeigen weiterleuchten, liegt ein Routerfehler vor.

Wenn sämtliche Anzeigen eine Minute nach Einschalten des Routers immer noch leuchten, sollten Sie die folgenden Schritte durchführen:

- Schalten Sie das Gerät aus, um zu sehen, ob der Fehler nur vorübergehend aufgetreten ist.
- Setzen Sie die Konfiguration des Routers auf die Werkseinstellungen zurück. Dabei wird als IP-Adresse des Routers „192.168.1.1“ festgelegt. Eine Anleitung hierzu finden Sie im Abschnitt „Wiederherstellen von Werkseinstellungen und Passwort“ auf Seite 7-7.

Wenn der Fehler sich dadurch nicht beheben lässt, liegt möglicherweise ein Hardwarefehler vor. Wenden Sie sich an den technischen Support.

Die LAN- oder WAN-Portanzeige leuchtet nicht

Falls die LAN-Anzeigen oder die Internetanzeige nicht leuchten, wenn eine Netzwerkverbindung hergestellt wird, überprüfen Sie die folgenden Punkte:

- Das Netzwerkkabel muss fest in die Anschlüsse am Router und am Switch oder an der Workstation eingesteckt sein.
- Der angeschlossene Switch bzw. die Workstation muss eingeschaltet sein.
- Das richtige Kabel muss verwendet werden:
  - Stellen Sie die Verbindung zwischen Router-Internet-Port und Kabel- oder DSL-Modem mit dem Kabel her, das dem Modem beilag. Dieses Kabel kann ein handelsübliches Netzwerkkabel oder ein Crossover-Kabel sein.

Netzwerkkonfigurationsoberfläche

Wenn Sie nicht über einen Computer im lokalen Netzwerk auf die Netzwerkkonfigurationsoberfläche zugreifen können, überprüfen Sie die folgenden Punkte:

- Überprüfen Sie die Netzwerkverbindung zwischen dem Computer und dem Router wie im vorigen Abschnitt beschrieben.
- Vergewissern Sie sich, dass die IP-Adresse des Computers zum selben Subnetz gehört wie der Router. Wenn Sie das empfohlene Adressenschema verwenden, sollte die IP-Adresse des Computers im Bereich von 192.168.1.2 bis 192.168.1.254 liegen. Wie Sie die IP-Adresse Ihres Computers herausfinden, erfahren Sie im Abschnitt „Überprüfen der TCP/IP-Eigenschaften“ auf Seite C-8 bzw. „Überprüfen der TCP/IP-Eigenschaften bei Apple-Computern“ auf Seite C-19. Konfigurieren Sie Ihren Computer gemäß den Anweisungen in Anhang C.

  Hinweis: Wird als IP-Adresse des Computers „169.254.x.y“ angezeigt? Neuere Versionen von Windows und MacOS erstellen eine IP-Adresse und weisen diese zu, wenn der Computer keinen DHCP-Server erreichen kann. Diese automatisch erstellten IP-Adressen liegen im Bereich 169.254.x.y. Wenn die IP-Adresse Ihres Computers in diesem Bereich liegt, sollten Sie die Verbindung vom Computer zum Router überprüfen und den Computer neu starten.
- Wenn die IP-Adresse Ihres Computers sich geändert hat und Sie die aktuelle IP-Adresse nicht kennen, setzen Sie die Konfiguration des Routers auf die Werkseinstellungen zurück. Dabei wird als IP-Adresse des Routers „192.168.1.1“ festgelegt. Eine Anleitung hierzu finden Sie im Abschnitt „Wiederherstellen von Werkseinstellungen und Passwort“ auf Seite 7-7.
- Vergewissern Sie sich, dass bei Ihrem Browser Java, JavaScript und ActiveX aktiviert sind. Wenn Sie den Internet Explorer verwenden, klicken Sie auf **Aktualisieren**, um sicherzugehen, dass das Java-Applet geladen wurde.
- Schließen Sie den Browser und starten Sie ihn erneut.
- Vergewissern Sie sich, dass Sie die korrekten Anmeldedaten verwenden. Die Werkseinstellungen sind wie folgt: Der Benutzername lautet „admin“ und das Passwort „password“. Achten Sie darauf, dass beim Eingeben dieser Daten die Feststelltaste nicht aktiviert ist.

Wenn der Router die über die Netzwerkkonfigurationsoberfläche vorgenommenen Änderungen nicht speichert, überprüfen Sie die folgenden Punkte:

- Beim Ändern der Konfigurationseinstellungen müssen Sie auf die Schaltfläche **Übernehmen** klicken, bevor Sie zu einem anderen Menü oder einer anderen Registerkarte wechseln. Anderenfalls gehen Ihre Änderungen verloren.
- Klicken Sie im Webbrowser auf die Schaltfläche **Aktualisieren** bzw. **Erneut laden**. Es kann sein, dass die Änderungen vorgenommen wurden, aber nicht angezeigt werden, da im Cache des Webbrowsers noch die alte Konfiguration gespeichert ist.

Internetverbindung

Wenn Ihr Router nicht auf das Internet zugreifen kann, sollten Sie zunächst feststellen, ob der Router eine WAN-IP-Adresse vom Internetdienstanbieter beziehen kann. Wurde Ihnen keine statische IP-Adresse zugewiesen, muss der Router eine IP-Adresse vom Internetdienstanbieter anfordern. Mit Hilfe der Konfigurationsoberfläche können Sie überprüfen, ob die Anforderung erfolgreich war.

So überprüfen Sie die WAN-IP-Adresse:

1. Starten Sie den Browser und besuchen Sie eine externe Website, z. B. www.netgear.de.
2. Rufen Sie das Hauptmenü der Routerkonfiguration unter *http://www.routerlogin.net* auf.
3. Wählen Sie unter „Wartung“ die Option **Routerstatus**.
4. Überprüfen Sie, ob für den WAN-Port eine IP-Adresse angezeigt wird. Wenn als Adresse „0.0.0.0“ angezeigt wird, hat der Internetdienstanbieter dem Router keine IP-Adresse zugewiesen.

Wenn Ihr Router keine IP-Adresse vom Internetdienstanbieter beziehen kann, müssen Sie u. U. das Kabel- oder DSL-Modem zwingen, den neuen Router zu erkennen, indem Sie die folgenden Schritte durchführen:

1. Schalten Sie das Kabel- oder DSL-Modem aus.
2. Schalten Sie den Router aus.
3. Warten Sie fünf Minuten und schalten Sie dann das Kabel- oder DSL-Modem wieder ein.
4. Wenn die Anzeigen des Modems erkennen lassen, dass es wieder mit dem Internetdienstanbieter synchronisiert ist, starten Sie den Router neu.
5. Starten Sie anschließend auch den Computer neu.

Wenn der Router immer noch keine IP-Adresse vom Internetdienstanbieter beziehen kann, kann dies folgende Ursachen haben:

- Vielleicht ist für Ihren Internetdienstanbieter ein Anmeldeprogramm erforderlich. Erkundigen Sie sich beim Internetdienstanbieter, ob Sie PPP over Ethernet (PPPoE) oder ein anderes Anmeldeprotokoll benötigen.
- Wenn eine Anmeldung beim Internetdienstanbieter erforderlich ist, haben Sie vielleicht den Benutzernamen oder das Passwort falsch eingegeben.
- Der Internetdienstanbieter überprüft vielleicht den Hostnamen des Computers. Geben Sie im Menü „Grundeinstellungen“ unter **Kontoname** den Computer-Hostnamen des Internetkontos ein.
- Der Internetdienstanbieter erlaubt nur einer MAC-Adresse den Verbindungsaufbau zum Internet und überprüft die MAC-Adresse des Computers. In diesem Fall haben Sie zwei Möglichkeiten:

Teilen Sie dem Internetdienstanbieter mit, dass Sie ein neues Netzwerkgerät angeschafft haben, und bitten Sie darum, die MAC-Adresse des Routers zu verwenden.

ODER

Konfigurieren Sie Ihren Router so, dass er seine MAC-Adresse fälscht, indem er die des Computers verwendet. Dies können Sie im Menü „Grundeinstellungen“ vornehmen. Nähere Informationen finden sie im Abschnitt „So umgehen Sie den Konfigurationsassistenten“ auf Seite 3-8.

Wenn Ihr Router eine IP-Adresse erhält, Sie aber dennoch keine Webseiten aus dem Internet anzeigen können, kann dies folgende Ursachen haben:

- Ihr Computer erkennt keine DNS-Serveradressen.

  Ein DNS-Server ist ein Host im Internet, der Internetnamen (z. B. www-Adressen) in numerische IP-Adressen umwandelt. Normalerweise stellt der Internetdienstanbieter Ihnen die Adressen von einem oder zwei DNS-Servern automatisch zur Verfügung. Wenn Sie bei der Konfiguration des Routers eine DNS-Adresse eingegeben haben, starten Sie den Computer neu und überprüfen Sie die DNS-Adresse. Eine Anleitung dazu finden Sie im Abschnitt „Installieren oder Überprüfen der Windows-Netzwerkkomponenten“ auf Seite C-9. Sie können die DNS-Adressen aber auch manuell auf dem Computer konfigurieren. Hinweise dazu finden Sie in der Dokumentation zu Ihrem Betriebssystem.

- Der Router ist auf dem Computer nicht als TCP/IP-Gateway konfiguriert.

  Wenn der Computer seine Daten über DHCP vom Router bezieht, starten Sie den Computer neu und überprüfen Sie die Gateway-Adresse. Eine Anleitung dazu finden Sie im Abschnitt „Installieren oder Überprüfen der Windows-Netzwerkkomponenten“ auf Seite C-9.

TCP/IP-Netzwerke mit einem Ping-Dienstprogramm prüfen

Die meisten TCP/IP-Terminals und Router enthalten ein Ping-Dienstprogramm, das ein Echo-Request-Paket an das angegebene Gerät sendet. Das Gerät antwortet dann mit einem Echo-Reply. Die Fehlersuche in TCP/IP-Netzwerken wird durch die Verwendung des Ping-Dienstprogramms auf den Computern oder Workstations sehr erleichtert.

Testen des LAN-Pfads zum Router

Sie können vom Computer aus ein Ping-Signal an den Router senden, um zu überprüfen, ob der LAN-Pfad zum Router korrekt eingerichtet ist.

So senden Sie von einem Computer mit Windows 95 oder höher ein Ping-Signal an den Router:

1. Klicken Sie auf der Windows-Symbolleiste auf die Schaltfläche **Start** und wählen Sie **Ausführen**.
2. Geben Sie im Eingabefeld „ping“ gefolgt von der IP-Adresse des Routers ein. Beispiel:

   ```
   ping 192.168.1.1
   ```

3. Klicken Sie auf **OK**.

   Daraufhin sollte eine Nachricht wie die folgende angezeigt werden:

   ```
   Pinging <IP-Adresse> with 32 bytes of data
   ```

   Wenn der Pfad funktioniert, wird diese Nachricht angezeigt:

   ```
   Reply from <IP-Adresse>: bytes=32 time=NN ms TTL=xxx
   ```

   Wenn der Pfad nicht funktioniert, wird diese Nachricht angezeigt:

   ```
   Request timed out
   ```

   Wenn der Pfad nicht richtig funktioniert, könnte eines der folgenden Probleme vorliegen:

   - Fehlerhafte physikalische Verbindung
     - — Vergewissern Sie sich, dass die LAN-Port-LED leuchtet. Falls die LED nicht leuchtet, befolgen Sie die Anweisungen im Abschnitt „Die LAN- oder WAN-Portanzeige leuchtet nicht“ auf Seite 7-2.
     - — Vergewissern Sie sich, dass die Verbindungs-LEDs für die Netzwerkkarten- und Switch-Ports, die mit der Workstation und dem Router verbunden sind, leuchten.
   - Fehlerhafte Netzwerkkonfiguration
     - — Vergewissern Sie sich, dass die Treiber für die Netzwerkkarte sowie die TCP/IP-Software auf dem Computer bzw. der Workstation installiert und richtig konfiguriert sind.
     - — Vergewissern Sie sich, dass die IP-Adressen des Routers und der Workstation richtig sind und dass die Adressen zum selben Subnetz gehören.

Testen des Pfads vom Computer zu einem entfernten Gerät

Nachdem Sie sich vergewissert haben, dass die LAN-Pfade einwandfrei funktionieren, sollten Sie den Pfad vom Computer zu einem entfernten Gerät testen. Geben Sie im Windows-Menü „Ausführen“ die folgende Anweisung ein:

```
PING -n 10 <IP-Adresse>
```

Setzen Sie dabei anstelle von *<IP-Adresse>* die IP-Adresse eines entfernten Geräts (z. B. des DNS-Servers des Internetdienstanbieters) ein.

Wenn der Pfad einwandfrei funktioniert, werden dieselben Antworten wie im vorigen Abschnitt angezeigt. Falls Sie keine Antworten erhalten, überprüfen Sie Folgendes:

— Ihr Computer muss eine IP-Adresse aus dem gleichen Subnetz wie der Router haben, der als Standardgateway eingerichtet ist. Wenn die IP-Konfiguration des Computers über DHCP erfolgt ist, werden diese Informationen nicht unter der Option **Netzwerk** in der **Systemsteuerung** angezeigt. Die IP-Adresse des Routers muss als Standardgateway eingerichtet sein. Eine Anleitung dazu finden Sie im Abschnitt „Installieren oder Überprüfen der Windows-Netzwerkkomponenten“ auf Seite C-9.

— Die Netzwerkadresse des Computers (der Abschnitt der IP-Adresse, der durch die Netzmaske festgelegt wird) muss sich von der Netzwerkadresse des entfernten Geräts unterscheiden.

— Das Kabel- oder DSL-Modem muss angeschlossen und in Betrieb sein.

— Wenn der Internetdienstanbieter dem Computer einen Hostnamen zugewiesen hat, geben Sie im Menü „Grundeinstellungen“ diesen Hostnamen im Feld **Kontoname** ein.

— Vielleicht akzeptiert der Internetdienstanbieter nur die MAC-Adresse eines einzigen Ihrer Computer und lehnt alle anderen ab. Viele Breitbandanbieter schränken den Zugang ein, indem sie nur Datenverkehr von der MAC-Adresse Ihres Breitbandmodems zulassen. Manche Internetdienstanbieter schränken den Zugang jedoch noch zusätzlich auf die MAC-Adresse eines einzelnen, an dieses Modem angeschlossenen Computers ein. Wenn dies der Fall ist, müssen Sie Ihren Router so konfigurieren, dass er die MAC-Adresse des berechtigten Computers dupliziert oder „fälscht“. Nähere Informationen finden sie im Abschnitt „So umgehen Sie den Konfigurationsassistenten“ auf Seite 3-8.

Wiederherstellen von Werkseinstellungen und Passwort

In diesem Abschnitt wird erklärt, wie Sie die Werkseinstellungen wiederherstellen (und das Administratorpasswort auf „password“ und die IP-Adresse auf „192.168.1.1“ zurücksetzen). Es gibt zwei Möglichkeiten zum Löschen der aktuellen Konfiguration und Wiederherstellen der Werkseinstellungen:

- Verwenden Sie die Funktion **Löschen** auf dem Router (siehe „Löschen der Konfiguration“ auf Seite 6-7).
- Betätigen Sie die Reset-Taste an der Rückseite des Routers. Wenden Sie diese Methode an, wenn Sie das Administratorpasswort oder die IP-Adresse nicht kennen.

Wenn Sie die Werkseinstellungen wiederherstellen möchten, ohne das Administratorkennwort oder die IP-Adresse zu kennen, müssen Sie die Reset-Taste an der Rückseite des Routers betätigen.

1. Halten Sie die Reset-Taste gedrückt, bis die Stromanzeige zu blinken beginnt (ungefähr 10 Sekunden).
2. Lassen Sie nun die Reset-Taste los und warten Sie, bis der Router neu gestartet wird.

   Wenn der Wireless Router nicht neu gestartet wird oder die Stromanzeige weiterblinkt oder gelb leuchtet, ist das Gerät eventuell defekt. Wenn der Fehler sich nicht beheben lässt, liegt möglicherweise ein Hardwarefehler vor. Wenden Sie sich an den technischen Support.

Probleme mit Datum und Uhrzeit

Das Menü „E-Mail“ im Bereich „Content-Filterung“ zeigt das aktuelle Datum sowie die Uhrzeit an. Der WPN824 Router nutzt das NTP-Protokoll (Network Time Protocol) zum Abruf der aktuellen Uhrzeit von einem der NTP-Server im Internet. Jeder Protokolleintrag wird mit Datum und Uhrzeit versehen. Im Zusammenhang mit Datum und Uhrzeit können u. a. die folgenden Probleme auftreten:

- Als Datum wird der 2. Januar 2003 angezeigt. Ursache: Der Router konnte noch keine Verbindung zu einem NTP-Server herstellen. Vergewissern Sie sich, dass die Einstellungen für den Internetzugang richtig konfiguriert sind. Wenn Sie die Konfiguration des Routers gerade erst abgeschlossen haben, warten Sie mindestens fünf Minuten und überprüfen Sie das Datum und die Uhrzeit dann erneut.
- Die Zeit weicht um eine Stunde ab. Ursache: Der Router stellt nicht automatisch auf Sommer-/Winterzeit um. Aktivieren oder deaktivieren Sie im Menü „E-Mail“ das Kontrollkästchen **Automatisch an Sommer-/Winterzeit anpassen**.

Kapitel 8
Erweiterte Routerkonfiguration

In diesem Kapitel erfahren Sie, wie Sie die erweiterten Merkmale Ihres RangeMax Wireless Router WPN824 konfigurieren. Diese Merkmale sind im Hauptmenü der Browser-Oberfläche unter „Erweitert“ zu finden.

	Hinweis: Wenn Sie sich nicht sehr gut mit Netzwerken und Routing auskennen, lesen Sie den Abschnitt Anhang B, „Netzwerke, Routing, Firewalls und Grundlagen“, um sich mit den Begriffen und Verfahren, die in diesem Kapitel vorkommen, vertraut zu machen.

Konfiguration der erweiterten WLAN-Einstellungen

Klicken Sie im Hauptmenü unter „Erweitert“ auf **WLAN-Konfiguration**, um den Bildschirm „Erweiterte WLAN-Einstellungen“ aufzurufen:

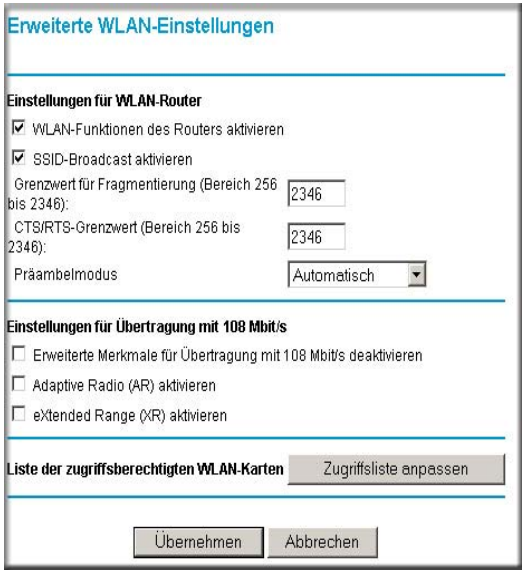


Abbildung 8-1: Die Seite „Erweiterte WLAN-Einstellungen“

Vorsicht: Der WLAN-Router ist bereits mit den optimalen Einstellungen konfiguriert. Änderungen an diesen Einstellungen dürfen nur auf ausdrückliche Anweisung des NETGEAR-Supports hin vorgenommen werden. Eine fehlerhafte Konfiguration kann dazu führen, dass der WLAN-Router nicht mehr funktioniert.

Programmieren Sie die erweiterten WLAN-Einstellungen wie folgt:

- **WLAN-Funktionen des Routers aktivieren**: Standardmäßig fungiert der Router als Access Point für ein WLAN; die entsprechenden Funktionen können jedoch auch deaktiviert werden. Die Wireless-LED an der Vorderseite des Routers zeigt an, ob dieser als Access Point fungiert. Wenn diese Option aktiviert ist, können andere WLAN-Geräte auf das Internet zugreifen. Wenn diese Option deaktiviert ist, können andere WLAN-Geräte nicht auf das Internet zugreifen.
- **SSID-Broadcast aktivieren**: Wenn diese Option aktiviert ist, überträgt der Router den Netzwerknamen (SSID) an alle Geräte im WLAN. Geräte, denen keine oder eine leere SSID zugewiesen wurde, können mit dieser SSID Verbindungen zum Access Point herstellen.
- **Grenzwert für Fragmentierung, CTS/RTS-Grenzwert, Präambelmodus**: Diese Einstellungen dienen nur zum Testen des WLAN und der erweiterten Konfiguration. Im normalen Betrieb sollten keine Änderungen an diesen Einstellungen vorgenommen werden.
- **Einstellungen für Übertragung mit 108 MBit/s**
  - **Erweiterte Merkmale für Übertragung mit 108 MBit/s deaktivieren**: Wenn diese Option deaktiviert ist, verwendet der WLAN-Router keine Datenkompression, kein Packet Bursting und keine Unterstützung für große Frames.
  - **Adaptive Radio aktivieren**: Das Merkmal Adaptive Radio (AR) steht zur Verfügung, wenn in den WLAN-Einstellungen der dynamische Übertragungsmodus 108 MBit/s automatisch angegeben wurde. Wenn dieses Merkmal aktiviert ist, wird automatisch in einen standardmäßigen 802.11-Modus (g oder b) mit niedrigerer Übertragungsgeschwindigkeit gewechselt, wenn ein anderes WLAN in der näheren Umgebung einen angrenzenden Kanal verwendet. Nur wenn keine angrenzenden Kanäle von anderen WLANs verwendet werden, erfolgt die Datenübertragung mit vollen 108 MBit/s. Da bei WLAN-Produkten von NETGEAR mit Unterstützung für 108 MBit/s ohnehin nur minimale Interferenzen mit benachbarten Netzwerken auftreten, ist das Merkmal Adaptive Radio standardmäßig deaktiviert.
  - **eXtended Range aktivieren**: eXtended Range (XR) ist eine Technik, die deutlich höhere WLAN-Reichweiten als herkömmliche 802.11-Verfahren und verlässliche Verbindungen selbst bei geringer Signalstärke ermöglicht. Produkte mit XR-Unterstützung erfordern keine zusätzliche Konfiguration durch den Anwender und sind uneingeschränkt mit den 802.11-Standards kompatibel.
- **Liste der zugriffsberechtigten WLAN-Karten**: Standardmäßig kann jeder WLAN-fähige Computer mit der richtigen SSID auf das WLAN zugreifen. Zur Erhöhung der Sicherheit können Sie den WLAN-Zugang auf einzelne Computer mit vorgegebenen MAC-Adressen beschränken.

Liste der zugriffsberechtigten WLAN-Karten

Auf der Seite „WLAN-Karten einrichten“ finden Sie eine Liste der WLAN-fähigen Computer, deren MAC-Adressen für den Zugriff auf den Router freigegeben wurden. Ob diese Computer auf das WLAN zugreifen können, hängt außerdem von den Einstellungen für SSID und Sicherheitsoptionen auf der Seite „WLAN-Konfiguration“ ab.

Klicken Sie im Menü „WLAN-Konfiguration“ auf die Schaltfläche **Zugriffsliste anpassen**, um zur Liste der zugriffsberechtigten WLAN-Karten zu gelangen und diese zu bearbeiten:

Abbildung 8-2: Der Bildschirm „Liste der zugriffsberechtigten WLAN-Karten“

Programmieren Sie die Liste der zugriffsberechtigten WLAN-Karten wie folgt:

- **Zugriffssteuerung aktivieren**
  a. Klicken Sie auf das Kontrollkästchen **Zugriffssteuerung aktivieren**, um den WLAN-Zugang auf Computer mit bestimmten MAC-Adressen zu beschränken
  b. Klicken Sie auf die Schaltfläche **Übernehmen**, um die Einstellungen zu speichern und zur Seite „WLAN-Konfiguration“ zurückzukehren.

  Hinweis: Wenn Sie die Option **Zugriffssteuerung aktivieren** wählen, die Liste für die Zugriffssteuerung jedoch keine Einträge enthält, kann von keinem Computer aus auf das WLAN zugegriffen werden.
- So richten Sie die Liste für die Zugriffssteuerung ein:
  a. Klicken Sie auf die Schaltfläche **Hinzufügen**, um zum Menü „Verfügbare WLAN-Karten“ zu gelangen (siehe Abbildung 8-3). Hier finden Sie eine Liste der verfügbaren WLAN-Karten mit den jeweiligen MAC-Adressen.
  b. Wenn der gewünschte Computer in der Liste angezeigt wird, können Sie dessen MAC-Adresse in das Eingabefeld übernehmen, indem Sie auf die entsprechende Optionsschaltfläche klicken. Sie können die MAC-Adresse des zugriffsberechtigten Computers auch manuell eingeben. Bei den meisten WLAN-Geräten ist die MAC-Adresse auf einem Aufkleber auf der Unterseite angegeben.
  c. Wenn kein Gerätename angezeigt wird, können Sie einen beschreibenden Namen für den hinzuzufügenden Computer eingeben.

d. Nachdem Sie die MAC-Adresse eingegeben haben, klicken Sie auf **Hinzufügen**, um zur Liste für die Zugriffssteuerung zurückzukehren.

Hinweis: Wiederholen Sie die Schritte a bis d für jeden zugriffsberechtigten Computer.

e. Klicken Sie auf **Zugriffssteuerung aktivieren**.

f. Klicken Sie auf die Schaltfläche **Übernehmen**, um die Einstellungen zu speichern und zur Seite „WLAN-Konfiguration“ zurückzukehren.

WLAN-Karten einrichten

Der Bildschirm „WLAN-Karten einrichten“ wird durch Klicken auf **Hinzufügen** im Menü „Liste der zugriffsberechtigten WLAN-Karten“ aufgerufen (siehe „Liste der zugriffsberechtigten WLAN-Karten“ auf Seite 8-3):

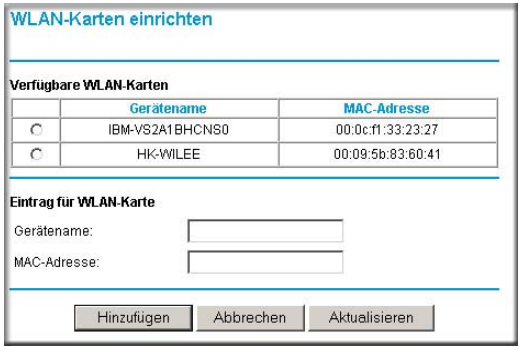


Abbildung 8-3: Der Bildschirm „WLAN-Karten einrichten“

Programmieren Sie das Menü „WLAN-Karten einrichten“ wie folgt:

- **Verfügbare WLAN-Karten**: In der Liste **Verfügbare WLAN-Karten** werden alle verfügbaren Computer mit WLAN-Unterstützung und deren MAC-Adressen angezeigt.

  Wenn der gesuchte Computer in der Liste **Verfügbare WLAN-Karten** angezeigt wird, können Sie durch Klicken auf die entsprechende Optionsschaltfläche dessen MAC-Adresse in das Eingabefeld übernehmen. Wenn der gesuchte Computer nicht angezeigt wird, können Sie auf die Schaltfläche **Aktualisieren** klicken, um die Liste der verfügbaren Computer mit WLAN-Unterstützung zu aktualisieren. Wenn der gesuchte Computer noch immer nicht angezeigt wird, können Sie die MAC-Adresse auch manuell eingeben. Gehen Sie dabei wie im Folgenden beschrieben vor.

- **Eintrag für WLAN-Karte**: Wenn in der Liste **Verfügbare WLAN-Karten** keine Computer mit WLAN-Unterstützung angezeigt werden, können Sie den Gerätenamen und die MAC-Adresse des zugriffsberechtigten Computers manuell eingeben.

Hinweis: Die MAC-Adresse ist eine zwölfstellige Zeichenfolge, die nur aus den Zeichen 0–9 und A–F besteht und manchmal durch Doppelpunkte unterteilt ist (z. B.: 00:09:AB:CD:EF:01). Bei den meisten WLAN-Geräten können Sie die MAC-Adresse einem Aufkleber an der Unterseite entnehmen.

Konfiguration von Port-Triggering und Portweiterleitung

Das Port-Triggering ist ein erweitertes Merkmal, das die Verwendung von Spielen und anderen Internetanwendungen erleichtert. Die Portweiterleitung ist von ihren Funktionen her mit dem Port-Triggering vergleichbar; sie ist jedoch statisch und unterliegt gewissen Einschränkungen.

Hinweis: Wenn Sie Anwendungen wie Multi-Player-Games, Peer-to-Peer-Verbindungen und Echtzeitkommunikation (z. B. Instant Messaging oder die Remoteunterstützung von Windows XP) verwenden, sollten Sie auch UPnP aktivieren. Befolgen Sie dazu die Anweisungen unter „Verwendung von Universal Plug and Play (UPnP)“ auf Seite 8-20.

Beim Port-Triggering wird ein Port vorübergehend für ankommenden Datenverkehr geöffnet; hierbei braucht die IP-Adresse nicht vom Server im Internet verfolgt zu werden, wenn diese beispielsweise per DHCP geändert wird.

Beim Port-Triggering wird der abgehende Datenverkehr überwacht. Wenn einer der Computer in Ihrem Netzwerk über einen Ausgangs-Port Daten sendet, speichert der Router dessen IP-Adresse und „triggert“ den entsprechenden Eingangs-Port. Am getriggerten Port eintreffende Daten werden dann an den Computer weitergeleitet, von dem auch die abgehenden Daten für diesen Port stammen.

Mit den Einstellungen auf der Seite „Port-Triggering“ können Sie lokalen Computern die Nutzung verschiedener Online-Spiele (wie Quake III) und Internetanwendungen (wie CUseeMe) ermöglichen.

Die Portweiterleitung eignet sich hingegen eher für ständige Angebote wie FTP und HTTP. Anforderungen aus dem Internet werden an den Server übermittelt, für den eine Weiterleitung des jeweiligen Ports eingerichtet wurde. Beim Port-Triggering werden hingegen Anforderungen aus dem Internet nur dann weitergeleitet, wenn der entsprechende Port zuvor „getriggert“ wurde. Das Port-Triggering eignet sich beispielsweise für die Nutzung von Chatforen und Online-Spielen.

Abbildung 8-4: Das Menü „Port-Triggering“

Hinweis: Wenn Sie das Kontrollkästchen **Port-Triggering deaktivieren** markieren, nachdem Sie das Port-Triggering konfiguriert haben, wird das Port-Triggering deaktiviert, doch die Port-Triggering-Konfigurationsdaten, die Sie dem Router hinzugefügt haben, bleiben erhalten, auch wenn sie nicht verwendet werden.

- **Leerlaufzeit für Port-Triggering**: Geben Sie einen Wert von bis zu 9999 Minuten ein. Die Leerlaufzeit für das Port-Triggering bestimmt, wie lange ein getriggerter Eingangs-Port geöffnet bleibt, wenn keine weiteren Daten über diesen Port übertragen werden. Wenn die Zeitspanne, in der keine Daten über den betreffenden Eingangs-Port mehr übertragen werden, die angegebene Leerlaufzeit erreicht, wird der Port geschlossen.
- **Für Online-Spiele und Internetanwendungen**: Zunächst müssen Sie wissen, welchen Dienst, welche Anwendung oder welches Spiel Sie konfigurieren möchten. Außerdem benötigen Sie die Adresse des Ausgangs-Ports (Triggering-Port), den das Spiel oder die Anwendung verwendet.

So richten Sie einen Computer für die Nutzung von Online-Spielen oder einer Internetanwendung ein:

1. Klicken Sie auf **Hinzufügen**.

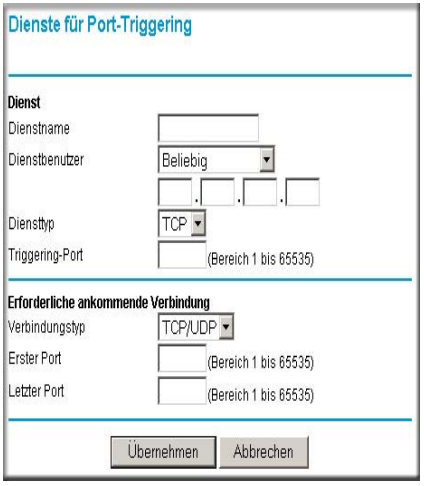


Abbildung 8-5: Das Menü zum Hinzufügen von Port-Triggering-Diensten

2. Geben Sie den Dienstnamen in das entsprechende Feld ein.
3. Wählen Sie unter **Dienstbenutzer** die Option **Beliebig** (Standardeinstellung), wenn dieser Dienst allen Benutzern im Netzwerk zur Verfügung stehen soll. Wählen Sie ansonsten **Einzelne Adresse** und geben Sie die IP-Adresse eines einzelnen Computers ein, wenn nur dieser eine Computer diesen Dienst nutzen soll.
4. Wählen Sie den **Diensttyp**.
5. Geben Sie im Feld **Triggering-Port** die Nummer des Ausgangs-Ports ein.
6. Füllen Sie die Felder **Verbindungstyp**, **Erster Port** und **Letzter Port** aus. Die entsprechenden Angaben finden Sie im Handbuch zum Spiel oder zur Anwendung oder auf der Website des Herstellers.
7. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

Konfiguration der Portweiterleitung an lokale Server

Der Router lässt Ihr gesamtes lokales Netzwerk als einen einzigen Computer im Internet erscheinen. Sie können jedoch trotzdem einen lokalen Server (z. B. einen Web- oder Spieleserver) im Internet anzeigen und verfügbar machen. Dies kann im Menü „Portweiterleitung“ eingestellt werden. Klicken Sie dazu im Hauptmenü der Browser-Oberfläche unter „Erweitert“ auf **Portweiterleitung** (Port Forwarding), um das unten abgebildete Menü „Portweiterleitung“ zu öffnen.

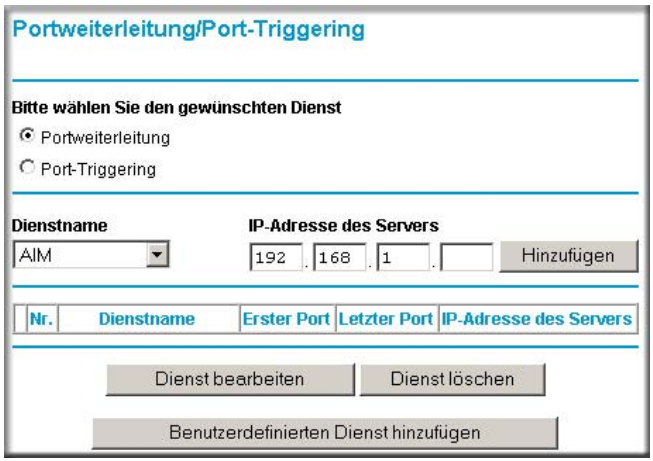


Abbildung 8-6: Das Menü „Portweiterleitung“

Mit dem Menü „Portweiterleitung“ können Sie den Router so konfigurieren, dass eingehende Protokolle an Computer in Ihrem lokalen Netzwerk weitergeleitet werden. Neben Servern für bestimmte Anwendungen können Sie dort auch einen DMZ-Standardserver (Exposed Host) festlegen, an den alle eingehenden Protokolle weitergeleitet werden. Der DMZ-Server wird im Menü „WAN-Konfiguration“ konfiguriert. (Siehe „WAN-Konfigurationsoptionen“ auf Seite 8-11.)

Ermitteln Sie zunächst, welche Art von Dienst, Anwendung oder Spiel Sie bereitstellen möchten und wie die IP-Adresse des Computers lautet, der den jeweiligen Dienst bereitstellen soll. Die IP-Adresse des Computers darf sich nicht ändern. So konfigurieren Sie die Portweiterleitung an einen lokalen Server:

Hinweis: Verwenden Sie die Adressreservierungsfunktion des WPN824 Routers, damit einem Computer immer dieselbe IP-Adresse zugewiesen wird. Eine Anleitung zur Verwendung reservierter IP-Adressen finden Sie unter „Reservieren von Adressen“ auf Seite 8-16.

1. Wählen Sie im Feld mit den Diensten und Spielen den Dienst bzw. das Spiel aus, das in Ihrem Netzwerk gehostet werden soll. Sollte der Dienst nicht in der Liste angezeigt werden, finden Sie im folgenden Abschnitt, „Hinzufügen eines benutzerdefinierten Dienstes“, weitere Informationen.
2. Geben Sie die IP-Adresse des lokalen Servers in das entsprechende Server-IP-Adressfeld ein.
3. Klicken Sie auf die Schaltfläche **Hinzufügen**.

Hinzufügen eines benutzerdefinierten Dienstes

Zum Definieren von Diensten, Spielen oder Anwendungen, die nicht in der Liste von Diensten und Spielen angezeigt werden, benötigen Sie die Portnummern des jeweiligen Dienstes. Sollten Ihnen diese nicht bekannt sein, wenden Sie sich an den Hersteller des Programms, das Sie verwenden möchten. Wenn Sie die Portnummern kennen, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf die Schaltfläche **Benutzerdefinierten Dienst hinzufügen**.

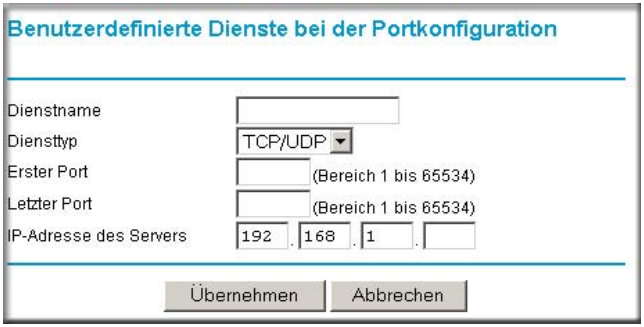


Abbildung 8-7: Das Menü „Benutzerdefinierte Dienste bei der Portkonfiguration“

2. Geben Sie den Dienstnamen in das entsprechende Feld ein.
3. Geben Sie die Nummer des ersten Ports im Portbereich in das Feld **Erster Port** ein.
   - Wenn die Anwendung nur einen Port verwendet, geben Sie dieselbe Portnummer in das Feld **Letzter Port** ein.
   - Wenn die Anwendung einen Bereich aus mehreren Ports verwendet, geben Sie die Nummer des letzten Ports in diesem Bereich in das Feld **Letzter Port** ein.
4. Geben Sie die IP-Adresse des Computers in das Feld **Server-IP-Adresse** ein.
5. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

Bearbeiten oder Löschen eines Portweiterleitungseintrags

So bearbeiten oder löschen Sie einen Portweiterleitungseintrag:

1. Klicken Sie in der Tabelle auf die Schaltfläche neben dem Dienstnamen.
2. Klicken Sie auf **Bearbeiten** oder **Löschen**.

Beispiel: Lokaler Web- und FTP-Server

Wenn ein lokaler Computer mit der privaten IP-Adresse „192.168.1.33“ als Web- und FTP-Server eingesetzt wird, muss das Portmenü so eingestellt werden, dass HTTP (Port 80) und FTP (Port 21) an die lokale Adresse „192.168.1.33“ weitergeleitet werden.

Um den Fernzugriff auf diesen Server über das Internet zu ermöglichen, müssen die Benutzer, die den Fernzugriff durchführen, die IP-Adresse kennen, die Ihnen von Ihrem Internetdienstanbieter zugewiesen wurde. Angenommen, diese Adresse lautet „172.16.1.23“. Dann kann ein Internetbenutzer auf Ihren Webserver zugreifen, indem er in der Adresszeile des Browsers „http://172.16.1.23“ eingibt. Die zugewiesene IP-Adresse kann dem Menüpunkt „Routerstatus“ entnommen werden. Sie wird dort als WAN-IP-Adresse angezeigt.

Bei dieser Art von Anwendung sollten Sie die folgenden Punkte beachten:

- Wenn bei Ihrem Konto die IP-Adresse dynamisch durch den Internetdienstanbieter vergeben wird, kann die Adresse sich von Zeit zu Zeit ändern, wenn der DHCP-Lease-Zeitraum abgelaufen ist oder die Verbindung zwischenzeitlich getrennt wurde.
- Wenn die IP-Adresse des lokalen Computers über DHCP vergeben wird, kann es sein, dass die IP-Adresse sich ändert, wenn der Computer neu gestartet wird. Sie können dies vermeiden, indem Sie den Router so konfigurieren, dass er diesem Computer eine Adresse fest reserviert.
- Lokale Computer müssen zum Zugriff auf diesen Server dessen lokale IP-Adresse verwenden (in diesem Beispiel „192.168.1.33“). Über die externe IP-Adresse (in diesem Beispiel „172.16.1.23“) können lokale Computer nicht auf den Server zugreifen.

Beispiel: Half Life, KALI oder Quake III mit mehreren Computern

So richten Sie einen weiteren Computer für Spiele wie Half Life, KALI oder Quake III ein:

1. Klicken Sie auf die Schaltfläche **Benutzerdefinierten Dienst hinzufügen**.
2. Geben Sie einen neuen Dienstnamen (z. B. KALI-Player2) in das entsprechende Feld ein.
3. Geben Sie die Nummer des ersten Ports im Portbereich in das Feld **Erster Port** ein.
   Erhöhen Sie bei den genannten Spielen die Portnummer bei jedem zusätzlichen Computer jeweils um eins. Wenn Sie beispielsweise bereits einen Computer für die Nutzung von Hexen II über Port 26900 eingerichtet haben, weisen Sie dem zweiten Computer die Portnummer 26901 und dem dritten Computer die Portnummer 26902 zu.

4. Geben Sie dieselbe Portnummer in das Feld **Letzter Port** ein.
5. Geben Sie im Feld „IP-Adresse des Servers“ die IP-Adresse des Computers ein.
6. Klicken Sie auf **Übernehmen**.

Nicht alle Online-Spiele und Videokonferenz-Anwendungen sind mit NAT kompatibel. Der WPN824 Router ist darauf programmiert, einige dieser Anwendungen zu erkennen und zu unterstützen, doch bei anderen Anwendungen können Probleme auftreten. In manchen Fällen ist es möglich, die Anwendung auf einem lokalen Computer fehlerfrei auszuführen, wenn die IP-Adresse dieses Computers als Standard im Ports-Menü eingegeben wird. Wenn ein lokaler Computer als Host für ein Spiel oder eine Videokonferenz eingesetzt werden soll, geben Sie die IP-Adresse dieses Computers als Standard ein.

WAN-Konfigurationsoptionen

Mit Hilfe der Optionen zur WAN-Konfiguration können Sie einen DMZ-Server konfigurieren, die MTU-Größe ändern und den Wireless Router so einrichten, dass er auf Ping-Anforderungen am WAN-Port reagiert. Diese Optionen werden unten beschrieben.

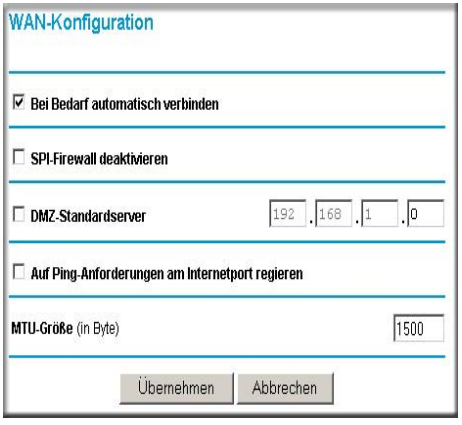


Abbildung 8-8: Das Menü „WAN-Konfiguration“

Bei Bedarf automatisch verbinden

Diese Option sollte normalerweise aktiviert sein. Nach dem Trennen der Internetverbindung wird diese automatisch neu aufgebaut, sobald für das Internet bestimmte Daten gesendet werden. Dadurch steht bei Bedarf immer eine Internetverbindung zur Verfügung, ohne dass unnötige Kosten entstehen. Dies ist von Vorteil, wenn Sie einen Internetdienst verwenden, der nach Verbindungszeit abrechnet. NETGEAR empfiehlt generell die Verwendung von Volumentarifen oder Flatrates, da einige Softwareprodukte – vom Anwender unbemerkt – selbständig Internetverbindungen aufbauen können, was bei zeitbasierter Abrechnung zu erhöhten Rechnungen führen kann. NETGEAR wird Schäden, die durch erhöhte Internetrechnungen entstehen, nicht ersetzen.

Wenn diese Option deaktiviert ist, müssen Sie Internetverbindungen manuell mit der Schaltfläche **Verbindungsstatus** auf dem Bildschirm „Routerstatus“ herstellen. Für manuell hergestellte Verbindungen gilt keine zeitliche Begrenzung; sie werden also nicht automatisch vom Router getrennt.

Deaktivieren der SPI-Firewall

Die SPI-Firewall (Stateful Packet Inspection) schützt das LAN vor Denial-of-Service-Angriffen. Diese Option sollte nur deaktiviert werden, wenn dies aus gegebenem Anlass erforderlich ist.

Einrichten eines Exposed Host (DMZ)

Ein Exposed Host, oft auch als „demilitarisierte Zone“ oder kurz „DMZ“ bezeichnet, kann bei Online-Spielen und Videokonferenz-Anwendungen, die nicht mit NAT kompatibel sind, sehr hilfreich sein. Der Router ist darauf programmiert, einige dieser Anwendungen zu erkennen und zu unterstützen, doch bei anderen Anwendungen können Probleme auftreten. In manchen Fällen ist es möglich, die Anwendung auf einem lokalen Computer fehlerfrei auszuführen, wenn die IP-Adresse dieses Computers als DMZ-Standardserver eingegeben wird.

Hinweis: DMZ-Server stellen ein Sicherheitsrisiko dar. Ein Computer, der als DMZ-Standardserver festgelegt wird, verliert einen Großteil des Firewall-Schutzes und ist Angriffen aus dem Internet ausgesetzt. Dies kann dazu führen, dass der DMZ-Server für Angriffe auf Ihr Netzwerk verwendet wird.

Über das Internet eingehende Daten werden normalerweise vom Router zurückgewiesen, wenn sie nicht von einem Ihrer lokalen Computer angefordert wurden oder zu einem der im Ports-Menü konfigurierten Dienste gehören. Statt diese Daten zurückzuweisen, können Sie sie an einen Computer in Ihrem Netzwerk weiterleiten. Dieser Computer ist der DMZ-Standardserver.

Im Menü „WAN-Konfiguration“ können Sie einen DMZ-Standardserver konfigurieren.

So richten Sie einen Computer oder Server als DMZ-Standardserver ein:

1. Klicken Sie im Hauptmenü unter „Erweitert“ auf den Link **WAN-Konfiguration**.
2. Geben Sie die IP-Adresse des Servers ein. Wenn Sie den DMZ-Server wieder entfernen möchten, ersetzen Sie einfach alle Ziffern der IP-Adresse durch Nullen.
3. Klicken Sie auf **Übernehmen**.

Ermöglichen von Reaktionen auf Ping-Anforderungen am Internet-WAN-Port

Wenn der Router auf Ping-Anforderungen aus dem Internet reagieren soll, aktivieren Sie das Kästchen **Auf Ping-Anforderungen am Internet-WAN-Port reagieren**. Diese Option sollte nur für Diagnosezwecke verwendet werden, da Ihr Router dadurch entdeckt werden kann. Aktivieren Sie dieses Kästchen nur, wenn ein dringender Grund dazu vorliegt.

Einstellen der MTU-Größe

Der MTU-Wert (Maximum Transmit Unit) beträgt normalerweise 1500 Byte für lokale Netzwerke, 1492 Byte für PPPoE-Verbindungen und 1436 für PPTP-Verbindungen. Bei einigen Internet-Serviceprovidern muss ein niedrigerer MTU-Wert eingestellt werden. Das ist jedoch nur in seltenen Fällen notwendig. Verwenden Sie diese Option daher nur, wenn Ihr Internetzugang eine abweichende Einstellung erfordert.

Wenn Datenpakete durch den Router gesendet werden, die die konfigurierte MTU-Größe überschreiten, werden diese in kleinere Datenpakete zerlegt, um den MTU-Anforderungen gerecht zu werden. So ändern Sie die MTU-Größe:

1. Geben Sie unter „MTU-Größe“ einen neuen Wert zwischen 64 und 1500 ein.
2. Klicken Sie zum Speichern der neuen Konfiguration auf **Übernehmen**.

Verwendung der LAN-IP-Konfigurationsoptionen

Zu den Menüpunkten im Bereich „Erweitert“ gehört auch die **LAN-IP-Konfiguration**. Damit können Sie LAN-IP-Dienste wie DHCP und RIP konfigurieren. Klicken Sie dazu im Hauptmenü der Browser-Oberfläche unter „Erweitert“ auf **LAN-IP-Konfiguration**, um das unten abgebildete Menü „LAN-IP-Konfiguration“ zu öffnen.

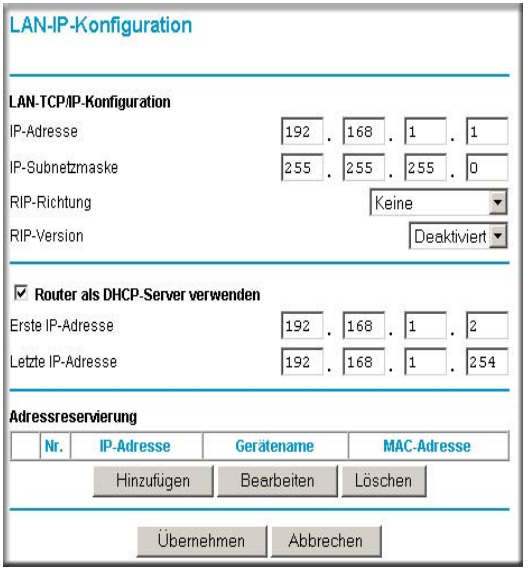


Abbildung 8-9: Das Menü „LAN-IP-Konfiguration“

LAN-TCP/IP-Parameter

Im Lieferzustand ist der Router so konfiguriert, dass er auf der LAN-Seite private IP-Adressen verwendet und als DHCP-Server fungiert. Die voreingestellte LAN-IP-Konfiguration des Routers sieht wie folgt aus:

- **LAN-IP-Adressen**: 192.168.1.1
- **Subnetzmaske**: 255.255.255.0

Diese Adressen gehören zu den von der IETF (Internet Engineering Task Force) für die Verwendung in privaten Netzwerken bestimmten privaten Adressen und sollten für die meisten Anwendungen geeignet sein. Wenn für Ihr Netzwerk ein anderes IP-Adressenschema erforderlich ist, können Sie die entsprechenden Änderungen in diesem Menü vornehmen.

Die LAN-IP-Parameter lauten:

- **IP-Adresse**
  Die LAN-IP-Adresse des Routers.
- **IP-Subnetzmaske**
  Die LAN-Subnetzmaske des Routers. Zusammen mit der IP-Adresse sorgt die IP-Subnetzmaske dafür, dass ein Gerät erkennen kann, bei welchen anderen Adressen es sich um lokale Adressen handelt und welche Adressen nur über ein Gateway oder einen Router zu erreichen sind.
- **RIP-Richtung**
  Mittels RIP (Routing Information Protocol) können Routinginformationen zwischen Routern ausgetauscht werden. Mit der Option „RIP-Richtung“ können Sie festlegen, auf welche Weise der Router RIP-Pakete sendet und empfängt. Die Vorgabe ist **Beide**.
  - Wenn Sie **Beide** oder **Nur abgehend** wählen, versendet der Router die Routingtabelle in regelmäßigen Abständen per Broadcast.
  - Wenn Sie **Beide** oder **Nur ankommend** wählen, übernimmt der Router eingehende Routinginformationen.
  - Wenn Sie **Keine** wählen, sendet der Router keine RIP-Pakete und ignoriert empfangene RIP-Pakete.
- **RIP-Version**
  Mit dieser Option können Sie das Format und die Broadcastmethode für den Versand von RIP-Paketen durch den Router steuern. (In Empfangsrichtung unterstützt der Router beide Formate.) Die Standardeinstellung für diese Option ist **RIP-1**.
  - RIP-1 wird praktisch von allen Netzwerkgeräten unterstützt. RIP-1 eignet sich für alle gängigen Netzwerkkonfigurationen.
  - Bei RIP-2 werden mehr Informationen übertragen. Bei RIP-2B erfolgt die Übertragung mittels Subnetz-Broadcasting.

Hinweis: Wenn Sie die LAN-IP-Adresse des Routers ändern, während Sie über den Browser verbunden sind, wird die Verbindung unterbrochen. Sie müssen dann eine Verbindung zur neuen IP-Adresse herstellen und sich erneut anmelden.

Einsatz des Routers als DHCP-Server

Der Router ist standardmäßig so konfiguriert, dass er als DHCP (Dynamic Host Configuration Protocol)-Server funktioniert und IP-, DNS-Server- und Standardgateway-Adressen an alle Computer, die mit dem LAN des Routers verbunden sind, vergeben kann. Als Standardgateway-Adresse wird die LAN-Adresse des Routers vergeben. Die IP-Adressenvergabe an die angeschlossenen Computer erfolgt aus einer Auswahl von IP-Adressen, die in diesem Menü festgelegt wird. Jede dieser Adressen wird vor der Vergabe getestet, um doppelte Adressen im LAN zu verhindern.

Für die meisten Anwendungen genügen die DHCP- und TCP/IP-Voreinstellungen des Routers. Unter „IP-Konfiguration über DHCP“ auf Seite B-10 finden Sie nähere Informationen zu DHCP und Hinweise zur Vergabe von IP-Adressen in Ihrem Netzwerk.

Wenn ein anderes Gerät in Ihrem Netzwerk als DHCP-Server eingesetzt wird oder Sie die Netzwerkeinstellungen auf allen Computern manuell vornehmen möchten, deaktivieren Sie das Kästchen **Router als DHCP-Server verwenden**. Lassen Sie es in allen anderen Fällen aktiviert.

Geben Sie die IP-Adressen an, die zur Vergabe verfügbar sein sollen, indem Sie die **Erste IP-Adresse** und die **Letzte IP-Adresse** festlegen. Diese Adressen sollten zum selben IP-Adressen-Subnetz gehören wie die LAN-IP-Adresse des Routers. Wenn Sie das Standard-Adressenschema verwenden, sollten Sie einen Bereich zwischen „192.168.1.2 “ und „192.168.1.253“ festlegen. Halten Sie jedoch ggf. einen Teil des Bereichs für Geräte mit festen IP-Adressen frei.

Der Router wird die folgenden Parameter an jedes LAN-Gerät, das eine DHCP-Anforderung absendet, übermitteln:

- Eine IP-Adresse aus dem festgelegten Bereich
- Subnetzmaske
- Gateway-IP-Adresse (die LAN-IP-Adresse des Routers)
- Primärer DNS-Server (wenn Sie im Menü „Grundeinstellungen“ eine primäre DNS-Adresse eingegeben haben – andernfalls die LAN-IP-Adresse des Routers)
- Sekundärer DNS-Server (wenn Sie im Menü „Grundeinstellungen“ eine sekundäre DNS-Adresse eingegeben haben)

Reservieren von Adressen

Wenn Sie für einen Computer im LAN eine reservierte IP-Adresse festlegen, wird diesem bei jedem Zugriff auf den DHCP-Server des Routers dieselbe IP-Adresse zugewiesen. Indem Sie einem Server eine reservierte IP-Adresse zuweisen, ist dieser immer unter derselben Adresse erreichbar.

So reservieren Sie eine IP-Adresse:

1. Klicken Sie auf die Schaltfläche **Hinzufügen**.
2. Geben Sie im Feld „IP-Adresse“ die IP-Adresse ein, die dem Computer oder Server zugewiesen werden soll.
   (Wählen Sie dazu eine IP-Adresse aus dem LAN-Subnetz des Routers aus, z. B. 192.168.1.X.)
3. Geben Sie die MAC-Adresse des Computers oder Servers ein.
   (Tipp: Wenn der Computer bereits in Ihrem Netzwerk registriert ist, können Sie seine MAC-Adresse aus dem Menü „Angeschlossene Geräte“ kopieren und hier einfügen.)
4. Klicken Sie auf **Übernehmen**, um die reservierte Adresse in die Tabelle aufzunehmen.

Hinweis: Die reservierte Adresse wird erst zugewiesen, wenn der Computer das nächste Mal mit dem DHCP-Server des Routers Kontakt aufnimmt. Starten Sie den Computer neu oder greifen Sie auf seine IP-Konfiguration zu und erzwingen Sie eine DHCP-Freigabe und -Erneuerung.

So können Sie eine reservierte Adresse bearbeiten oder löschen:

1. Klicken Sie auf die Schaltfläche neben der reservierten Adresse, die Sie bearbeiten oder löschen möchten.
2. Klicken Sie auf **Bearbeiten** oder **Löschen**.

Verwendung von dynamischen DNS-Diensten (DDNS)

Wenn Ihrem Netzwerk eine permanente IP-Adresse zugewiesen wurde, können Sie einen Domainnamen registrieren und diesen Namen über öffentliche Domain Name Server (DNS) mit Ihrer IP-Adresse verknüpfen lassen. Falls Ihr Internetzugang jedoch über dynamisch vergebene IP-Adressen funktioniert, können Sie nicht im Voraus sagen, wie Ihre IP-Adresse lauten wird. Zudem kann die Adresse sich häufig ändern. In diesem Fall können Sie einen kommerziellen dynamischen DNS-Dienst nutzen. Sie können dann Ihre Domain unter der IP-Adresse dieses Anbieters registrieren und für Ihre Domain bestimmten Datenverkehr an Ihre aktuelle IP-Adresse weiterleiten lassen.

Hinweis: Wenn Ihr Internetdienstanbieter private WAN-IP-Adressen vergibt (wie z. B. „192.168.x.y“ oder „10.x.y.z“), funktioniert der dynamische DNS-Dienst nicht, da eine Internet-Weiterleitung an private Adressen nicht möglich ist.

Der Router enthält einen Client, der eine Verbindung zu gängigen dynamischen DNS-Diensten herstellen kann. Sie können sich einen dieser Dienste aussuchen und ein Konto dafür einrichten lassen. Sobald sich die vom Internetdienstanbieter zugewiesene IP-Adresse ändert, kontaktiert Ihr Router automatisch den Anbieter des dynamischen DNS-Dienstes, meldet sich bei Ihrem Konto an und registriert die neue IP-Adresse.

Klicken Sie im Hauptmenü der Browseroberfläche unter „Erweitert“ auf **Dynamisches DNS**. So konfigurieren Sie das dynamische DNS:

1. Richten Sie ein Konto bei einem der Anbieter für dynamische DNS-Dienste ein, die im Feld **DDNS-Anbieter** angezeigt werden. Gehen Sie z. B. zu www.dyndns.org, wenn Sie ein Konto bei dyndns.org einrichten möchten.
2. Aktivieren Sie das Kästchen **DDNS-Dienst verwenden**.
3. Wählen Sie den Namen Ihres DDNS-Anbieters aus der entsprechenden Liste aus.
4. Geben Sie den Hostnamen (oder Domainnamen) ein, der Ihnen vom DDNS-Anbieter zugewiesen wurde.
5. Geben Sie den Benutzernamen für Ihr DDNS-Konto ein.
6. Geben Sie das Passwort (oder den Schlüssel) für Ihr DDNS-Konto ein.
7. Wenn Ihr DDNS-Anbieter für Ihre URL die Verwendung von Platzhaltern zulässt, können Sie zur Aktivierung dieser Funktion das Kästchen **Platzhalter verwenden** aktivieren.
   Die Platzhalter-Funktion ermöglicht es z. B., dass „*.yourhost.dyndns.org“ als Alias für dieselbe IP-Adresse wie „yourhost.dyndns.org“ akzeptiert wird.
8. Klicken Sie auf **Übernehmen**, um die Konfiguration zu speichern.

Konfiguration statischer Routen

Statische Routen liefern Ihrem Router zusätzliche Routinginformationen. Unter normalen Umständen verfügt der Router über ausreichende Informationen, wenn er für den Internetzugang konfiguriert wurde, und es müssen keine weiteren statischen Routen konfiguriert werden. Statische Routen müssen nur in Ausnahmefällen festgelegt werden, z. B. wenn Ihr Netzwerk mehrere Router oder IP-Subnetze enthält.

Klicken Sie dazu im Hauptmenü der Browser-Oberfläche unter „Erweitert“ auf **Statische Routen**, um das unten abgebildete Menü „Statische Routen“ zu öffnen.

Abbildung 8-10: Übersicht über die statischen Routen

So fügen Sie eine statische Route hinzu oder bearbeiten diese:

1. Klicken Sie auf die Schaltfläche **Hinzufügen**, um das Menü zum Hinzufügen und Bearbeiten zu öffnen.

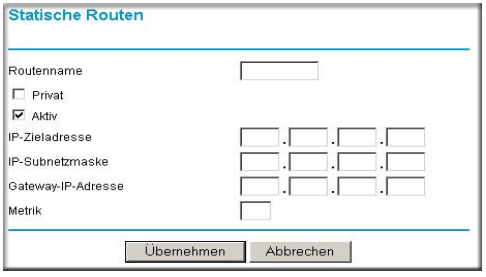


Abbildung 8-11. Das Menü zum Eingeben und Bearbeiten statischer Routen

2. Geben Sie im Feld **Routenname** unterhalb der Tabelle eine Bezeichnung für die Route ein. (Der Routenname hat nur beschreibende Funktion und kann frei gewählt werden.)
3. Wählen Sie **Privat**, wenn der Zugriff auf das LAN beschränkt werden soll. Die statische Route erscheint dann nicht im RIP.
4. Zum Aktivieren der Route wählen Sie **Aktiv**.
5. Geben Sie die **IP-Zieladresse** des Zielhosts für die Route ein.
6. Geben Sie die **IP-Subnetzmaske** für das Ziel ein.
   Wenn es sich dabei um einen einzelnen Host handelt, geben Sie „255.255.255.255“ als Ziel ein.
7. Geben Sie die **Gateway-IP-Adresse** ein; hierbei muss es sich um einen Router im selben LAN-Segment handeln.

8. Geben Sie im Feld **Metrik** einen Wert aus dem Bereich 1 bis 15 ein.
   Dieser Wert steht für die Anzahl der Router zwischen Ihrem Netzwerk und dem Ziel. In der Regel funktionieren die Werte „2“ und „3“; bei direkten Verbindungen sollte jedoch immer der Wert „1“ gewählt werden.
9. Klicken Sie auf **Übernehmen**, um die statische Route der Tabelle hinzuzufügen.

Im Folgenden finden Sie ein Beispiel für einen Fall, der den Einsatz einer statischen Route erforderlich macht:

- Ihr Hauptinternetzugang erfolgt über ein Kabelmodem, das Sie mit dem Internetdienstanbieter verbindet.
- Außerdem ist an Ihr Heimnetzwerk ein ISDN-Router angeschlossen, über den Sie eine Verbindung zu dem Unternehmen, für das Sie arbeiten, aufbauen. Die Adresse dieses Routers in Ihrem LAN lautet „192.168.1.100“.
- Die Adresse des Unternehmens ist „134.177.0.0“.

Bei der anfänglichen Konfiguration des Routers wurden zwei statische Routen erstellt. Es wurde eine Standardroute mit Ihrem Internetdienstanbieter als Gateway eingerichtet sowie eine zweite statische Route zu Ihrem lokalen Netzwerk für sämtliche Adressen des Typs „192.168.1.x“. Wenn Sie versuchen, mit dieser Konfiguration auf ein Gerät im 134.177.0.0-Netzwerk zuzugreifen, leitet Ihr Router diese Anforderung an den Internetdienstanbieter weiter. Der Internetdienstanbieter gibt diese Anforderung an das Unternehmen, für das Sie arbeiten, weiter, wo sie wahrscheinlich von der Unternehmensfirewall abgelehnt wird.

In diesem Fall müssen Sie eine statische Route festlegen und dem Router sagen, dass der Zugriff auf „134.177.0.0“ über den ISDN-Router mit der Adresse „192.168.1.100“ erfolgen soll. Die statische Route würde aussehen wie in Abbildung 8-11.

In diesem Beispiel gilt:

- Die Einträge in den Feldern **IP-Zieladresse** und **IP-Subnetzmaske** legen fest, dass diese statische Route für alle Adressen des Typs „134.177.x.x“ gilt.
- Der Wert im Feld **Gateway-IP-Adresse** gibt an, dass der gesamte Datenverkehr für diese Adressen an den ISDN-Router mit der Adresse „192.168.1.100“ weitergeleitet werden soll.
- Im Feld **Metrik** kann „1“ stehen, da der ISDN-Router sich innerhalb des LANs befindet.
- **Privat** wurde nur als Vorsichtsmaßnahme ausgewählt, falls RIP aktiviert ist.

Ermöglichen der Fernsteuerung

Auf dieser Seite können Sie Ihren Router so konfigurieren, dass ein oder mehrere Benutzer über das Internet die Geräteeinstellungen ändern, die Routersoftware aktualisieren sowie den Status des WPN824 Routers abfragen können.

	Hinweis: Geben Sie Ihren Router nur zur Fernsteuerung frei, wenn Sie zuvor das Standard-Konfigurationspasswort durch ein sicheres Passwort ersetzt haben. Das Passwort sollte idealerweise keine Wörter enthalten, die in irgendeiner Sprache im Wörterbuch stehen, und sollte aus Buchstaben (Groß- und Kleinbuchstaben), Ziffern und Symbolen zusammengesetzt sein. Ihr Passwort darf aus bis zu 30 Zeichen bestehen.

So konfigurieren Sie den Router für die Fernsteuerung:

1. Aktivieren Sie das Kontrollkästchen **Fernsteuerung aktivieren**.
2. Geben Sie an, welche externen Adressen Zugriff auf die Fernsteuerung des Routers erhalten sollen.

   Hinweis: Aus Sicherheitsgründen sollte der Fernzugriff auf einige wenige externe IP-Adressen beschränkt bleiben.

   a. Wenn jede beliebige IP-Adresse im Internet Zugriffsrechte erhalten soll, wählen Sie **Uneingeschränkt**.

   b. Wenn nur IP-Adressen eines bestimmten Bereichs Zugriffsrechte erhalten sollen, wählen Sie **IP-Adressbereich**. Geben Sie eine erste und eine letzte IP-Adresse ein, um den Bereich erlaubter Adressen festzulegen.

   c. Wenn nur eine einzige IP-Adresse im Internet die Zugriffsrechte erhalten soll, wählen Sie **Nur für diesen Computer**. Geben Sie die IP-Adresse ein, die die Zugriffsrechte erhalten soll.
3. Legen Sie die Portnummer fest, die für den Zugriff auf die Fernsteuerungsoberfläche verwendet werden soll.

   Dem HTTP-Dienst, über den der Zugriff per Webbrowser erfolgt, ist standardmäßig der Port 80 zugewiesen. Zur Erhöhung der Sicherheit weisen Sie am besten für den Fernzugriff per Internet auf den Router eine andere Portnummer zu. Wählen Sie eine Nummer im Bereich 1024 bis 65535; verwenden Sie jedoch keine Standard-Portnummern gängiger Internetdienste. Als Standardwert ist „8080“ eingestellt, ein gängiges Alias für HTTP.
4. Klicken Sie auf **Übernehmen**, um die Änderungen an den Router zu übermitteln.

Hinweis: Um über das Internet auf den Router zugreifen zu können, müssen Sie die WAN-IP-Adresse in die Adressleiste des Webbrowsers eingeben, gefolgt von einem Doppelpunkt (:) und der benutzerdefinierten Portnummer. Angenommen, Ihre externe IP-Adresse lautet „134.177.0.123“ und Sie verwenden Portnummer „8080“. Dann müssen Sie im Browser „http://134.177.0.123:8080“ eingeben.

Verwendung von Universal Plug and Play (UPnP)

Universal Plug and Play (UPnP) vereinfacht die Vernetzung von Geräten aller Art, beispielsweise von Internet-Geräten und Computern. UPnP-fähige Geräte erkennen die von anderen registrierten UPnP-Geräten im Netzwerk angebotenen Dienste automatisch.

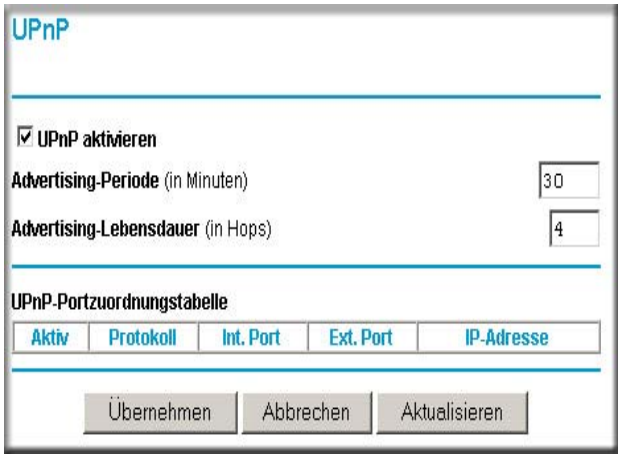


Abbildung 8-12. Das Menü „UPnP“

Klicken Sie im Hauptmenü der Browseroberfläche unter „Erweitert“ auf **UPnP**. Beachten Sie bei der Einrichtung von UPnP die folgenden Hinweise:

UPnP aktivieren: Die automatische Gerätekonfiguration per UPnP kann aktiviert oder deaktiviert werden. Standardmäßig ist UPnP aktiviert. Wenn UPnP deaktiviert ist, können andere Geräte die Ressourcen des Routers (wie z. B. die Portweiterleitung/Portzuordnung) nicht automatisch steuern.

Hinweis: Wenn Sie Anwendungen wie Multi-Player-Games, Peer-to-Peer-Verbindungen und Echtzeitkommunikation (z. B. Instant Messaging oder die Remoteunterstützung von Windows XP) verwenden, sollten Sie UPnP aktivieren.

Advertising-Periode: Die Advertising-Periode legt fest, wie oft die UPnP-Daten des Routers gesendet werden. Hier können Werte im Bereich 1 bis 1440 Minuten angegeben werden. Der Standardwert ist 30 Minuten. Kürzere Perioden stellen sicher, dass die Steuerungspunkte über aktuelle Informationen zum Gerätestatus verfügen, führen jedoch zu einem erhöhten Datenverkehr im Netzwerk. Bei längeren Perioden werden die Gerätestatusinformationen weniger oft aktualisiert; dafür verringert sich jedoch der Datenverkehr im Netzwerk erheblich.

Advertising-Lebensdauer: Die Advertising-Lebensdauer wird in Hops (Schritten) für jedes gesendete UPnP-Paket gemessen. Die Lebensdauer gibt die maximale Anzahl von Hops (Schritten) für die Weitergabe eines Broadcast-Pakets beim UPnP-Advertising an. Für die Anzahl der Hops können Werte im Bereich 1 bis 255 angegeben werden. Der Standardwert für die Advertising-Lebensdauer ist 4 Hops. Für Netzwerke in Privathaushalten ist dieser Wert in der Regel ausreichend. Wenn Sie feststellen, dass einige Geräte nicht aktualisiert oder nicht erreicht werden, sollten Sie einen geringfügig höheren Wert wählen.

UPnP-Portzuordnungstabelle: In der UPnP-Portzuordnungstabelle werden die IP-Adressen aller auf den Router zugreifenden UPnP-Geräte und die von diesen geöffneten Ports (intern und extern) angezeigt. Darüber hinaus können Sie der Tabelle die Typen der geöffneten Ports und deren Status (d. h. ob diese für die einzelnen IP-Adressen noch aktiv sind) entnehmen.

Anhang A
Technische Daten

Dieser Anhang enthält die technischen Daten zum RangeMax Wireless Router WPN824.

Kompatibilität mit Netzwerkprotokollen und Normen

Daten- und Routingprotokolle:	TCP/IP, RIP-1, RIP-2, DHCP PPP over Ethernet (PPPoE)

Netzteil

Nordamerika:	120 V, 60 Hz Eingangsleistung
Großbritannien, Australien:	240 V, 50 Hz Eingangsleistung
Europa:	230 V, 50 Hz Eingangsleistung
Japan:	100 V, 50/60 Hz Eingangsleistung
Alle Regionen (Ausgangsleistung):	12 V bei 1 A Ausgangsstrom, max. 22 W

Physikalische Daten

Abmessungen:	28 x 175 x 119 mm
Gewicht:	0,3 kg

Umgebungsdaten

Betriebstemperatur:	0–40 °C
Luftfeuchtigkeit:	90 % maximale relative Luftfeuchtigkeit, nicht kondensierend

Elektromagnetische Emissionen

Erfüllt folgende Anforderungen:	FCC Teil 15, Klasse B
	VCCI, Klasse B
	EN 55 022 (CISPR 22), Klasse B C-Tick N10947

Technische Daten zur Schnittstelle

LAN:	10BASE-T oder 100BASE-Tx, RJ-45
WAN:	10BASE-T oder 100BASE-Tx, RJ-45

Drahtlose Eigenschaften	
Drahtlose Datenübertragungsraten:	1, 2, 5,5, 6, 9, 12, 18, 24, 36, 48, 54 und 108 MBit/s Automatische Erkennung der Übertragungsrate
Frequenz:	2,4–2,5 GHz
Modulationsverfahren:	802.11b: Direct Sequence Spread Spectrum (DSSS) 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)
Höchstzahl an Computern pro WLAN:	Abhängig vom Umfang des WLAN-Datenverkehrs an jedem Netzwerkknoten. Normalerweise 30–70 Endgeräte.
Betriebsfrequenzbereiche:	2,412~2,462 GHz (USA) 2,457~2,462 GHz (Spanien) 2,412~2,484 GHz (Japan) 2,457~2,472 GHz (Frankreich) 2,412~2,472 GHz (Europa ETSI)
802.11-Verschlüsselungsverfahren:	64-Bit und 128-Bit WEP (Wired Equivalent Privacy) WPA-PSK (Wi-Fi Protected Access mit Pre-Shared Key)

Anhang B
Netzwerke, Routing, Firewalls und Grundlagen

Dieses Kapitel gibt einen Überblick über IP-Netzwerke, Routing und allgemeine Netzwerkfragen.

Weiterführende Dokumente

In diesem Anhang wird häufiger auf RFC-Dokumente mit weiteren Informationen verwiesen. „RFC“ steht für „Request For Comment“. RFCs werden von der Internet Engineering Task Force (IETF) herausgegeben, einer offenen Vereinigung, die für die Architektur und Funktionsweise des Internets zuständig ist. In den RFC-Dokumenten werden die Standardprotokolle und -verfahren für das Internet festgelegt. Diese Dokumente sind im Internet unter *www.ietf.org* zu finden. Zahlreiche andere Websites enthalten ebenfalls Auszüge und Querverweise auf diese Dokumente.

Grundlegende Routerkonzepte

In einem LAN (Local Area Network) können große Bandbreiten einfach und relativ preisgünstig bereitgestellt werden. Die Bereitstellung einer großen Bandbreite zwischen einem lokalen Netzwerk und dem Internet kann dagegen sehr kostspielig sein. Auf Grund dieser Kosten wird der Internetzugang in der Regel über eine langsamere WAN-Verbindung (Wide Area Network) hergestellt, z. B. über ein Kabel- oder DSL-Modem. Um eine optimale Ausnutzung der langsameren WAN-Verbindung zu gewährleisten, benötigt man einen Mechanismus, der den für das Internet bestimmten Datenverkehr auswählt und dafür sorgt, dass nur diese Daten übertragen werden. Die Auswahl und Weiterleitung dieser Daten wird von einem Router übernommen.

Was ist ein Router?

Ein Router ist ein Gerät, das den Datenverkehr zwischen Netzwerken weiterleitet. Die Weiterleitung erfolgt anhand der in den Daten enthaltenen Informationen aus der Vermittlungsschicht und der vom Router geführten Routingtabellen. In diesen Routingtabellen legt der Router ein logisches Abbild des gesamten Netzwerks an, indem er Daten sammelt und diese mit anderen Routern im Netzwerk austauscht. Anhand dieser Informationen wählt der Router dann den besten Pfad für die Weiterleitung des Netzwerkverkehrs.

Router unterscheiden sich in ihrer Leistung und ihrem Umfang, der Anzahl der unterstützten Routingprotokolle und der Arten von WAN-Verbindung, die sie unterstützen. Der RangeMax Wireless Router WPN824 ist ein kleiner Router für Bürozwecke, der das IP-Protokoll über eine Einzelbenutzer-Breitbandverbindung lenkt.

RIP (Routing Information Protocol)

Zu den Protokollen, mit deren Hilfe Router ein Abbild des Netzwerks aufbauen und aktualisieren, gehört das Routing Information Protocol (RIP). Mit Hilfe von RIPs senden Router sich gegenseitig in regelmäßigen Abständen Aktualisierungen zu und suchen nach Veränderungen, die in die Routingtabelle aufgenommen werden müssen.

Der WPN824 Router unterstützt sowohl das ältere Protokoll RIP-1 als auch das neuere RIP-2. Zu den Neuerungen von RIP-2 gehört die Unterstützung von Subnetz- und Multicast-Protokollen. RIP ist für die meisten in Privathaushalten eingesetzten Anwendungen nicht erforderlich.

IP-Adressen und das Internet

Da TCP/IP-Netzwerke in der gesamten Welt miteinander verbunden sind, benötigt jedes Gerät im Internet eine eindeutige Adresse. Nur so kann sichergestellt werden, dass gesendete Daten am vorgesehenen Ziel ankommen. Die Vergabe von Adressen erfolgt blockweise durch die IANA (Internet Assigned Numbers Authority). Einzelne Benutzer und kleinere Unternehmen und Organisationen können ihre Adressen entweder direkt von der IANA oder über einen Internetdienstanbieter beziehen. Sie können die IANA unter www.iana.org kontaktieren.

Das Internet Protocol (IP) verwendet eine 32-Bit-Adressstruktur. Die Adresse wird normalerweise in der Dezimalschreibweise (auch als Punktnotation bezeichnet) angegeben. Dabei werden die einzelnen Gruppen von jeweils acht Bit in dezimaler Form und durch Punkte getrennt angegeben.

So erscheint z. B. die folgende binäre Adresse

```
11000011 00100010 00001100 00000111
```

in der Regel als

```
195.34.12.7
```

Die zweite Version prägt sich besser ein und ist außerdem bequemer für die Eingabe.

Die 32 Bit der Adresse werden zudem in zwei Teile unterteilt: Der erste Teil der Adresse identifiziert das Netzwerk, der zweite Teil den Host-Knoten oder die Host-Station des Netzwerks. Der Trennpunkt zwischen dem ersten und zweiten Teil kann je nach Adressabschnitt und Anwendung unterschiedlich sein.

Es gibt fünf Standardklassen von IP-Adressen. Bei jeder dieser Adressklassen wird der Netzwerk- und Hostabschnitt der Adresse auf unterschiedliche Weise festgelegt, um die unterschiedliche Hostanzahl in Netzwerken zu berücksichtigen. Jede Adresse beginnt mit einem eindeutigen Bit-Muster, über das die TCP/IP-Software die Adressklasse identifizieren kann. Anhand der Adressklasse kann die Software den Hostabschnitt der Adresse ermitteln. Die folgende Abbildung zeigt die drei wichtigsten Adressklassen mit den jeweiligen Netzwerk- und Hostabschnitten.

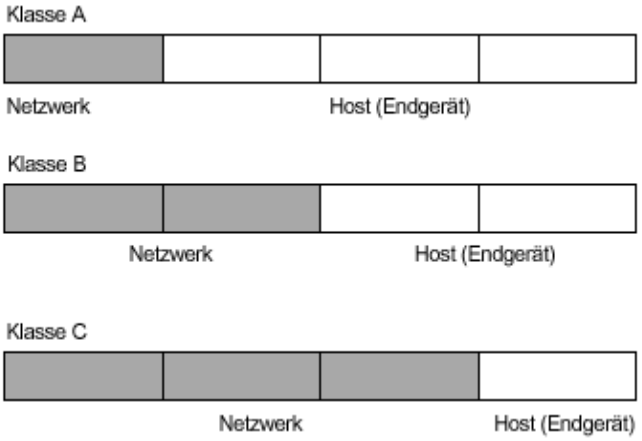


Abbildung B-1: Die drei wichtigsten Adressklassen

Die fünf Adressklassen sind:

- Klasse A
  Adressen der Klasse A lassen bis zu 16.777.214 Hosts in einem einzigen Netzwerk zu. Sie verwenden 8 Bit für die Netzwerknummer und 24 Bit für die Hostadresse. Die Adressen der Klasse A befinden sich in diesem Bereich:

  `1.x.x.x bis 126.x.x.x.`

- Klasse B
  Adressen der Klasse B lassen bis zu 65.354 Hosts in einem Netzwerk zu. Sie verwenden jeweils 16 Bit für die Netzwerknummer und die Hostadresse. Die Adressen der Klasse B befinden sich in diesem Bereich:

  `128.1.x.x bis 191.254.x.x.`

- Klasse C
  Adressen der Klasse C lassen bis zu 254 Hosts in einem Netzwerk zu. Sie verwenden 24 Bit für die Netzwerkadresse und 8 Bit für die Hostadresse. Die Adressen der Klasse C befinden sich in diesem Bereich:

  `192.0.1.x bis 223.255.254.x.`

- Klasse D
  Die Adressen der Klasse D werden für Multicasts (Übersenden von Nachrichten an mehrere Hosts) verwendet. Sie befinden sich in diesem Bereich:

  `224.0.0.0 bis 239.255.255.255.`

- Klasse E
  Die Adressen der Klasse E dienen experimentellen Zwecken.

Dank dieser Adressstruktur können IP-Adressen jedes physikalische Netzwerk und jeden Host in jedem physikalischen Netzwerk eindeutig identifizieren.

Als Netzwerkadresse für jeden eindeutigen Wert des Netzwerkabschnitts der Adresse wird die Basisadresse des Bereichs (mit lauter Nullen als Hostadresse) verwendet. Diese wird in der Regel nicht an einen Host zugewiesen. Die höchste Adresse des Bereichs (bei der die Hostadresse aus lauter Einsen – bzw. dem Wert 255 – besteht) wird ebenfalls nicht vergeben, sondern wird als Broadcast-Adresse verwendet. Über die Broadcast-Adresse kann ein Paket simultan an alle Hosts mit derselben Netzwerkadresse versendet werden.

Netzmaske

In den oben beschriebenen Adressklassen wird die Größe der beiden Abschnitte (Netzwerkadresse und Hostadresse) durch die Klasse festgelegt. Dieses Unterteilungsschema kann auch durch eine der IP-Adresse zugeordnete Netzmaske ausgedrückt werden. Über die 32 Bit lange Netzmaske lässt sich durch logische UND-Verknüpfung mit einer IP-Adresse die Netzwerkadresse ermitteln. Die Netzmasken für die Klassen A, B und C lauten z. B.: 255.0.0.0, 255.255.0.0 und 255.255.255.0.

Die IP-Adresse „192.168.170.237“ ist eine Adresse der Klasse C, deren Netzwerkabschnitt aus den vorderen 24 Bit besteht. Wenn diese Adresse, wie hier gezeigt, mit der Netzmaske für die Klasse C logisch mit UND verknüpft wird, bleibt nur der Netzwerkabschnitt der Adresse übrig:

```
11000000 10101000 10101010 11101101 (192.168.170.237)
```

verknüpft mit

```
11111111 11111111 11111111 00000000 (255.255.255.0)
```

ist gleich

```
11000000 10101000 10101010 00000000 (192.168.170.0)
```

Als kürzere Alternative zur Dezimalschreibweise kann die Netzmaske auch als Anzahl der Einsen von links gezählt angegeben werden. Diese Anzahl wird nach einem Backslash (/) an die IP-Adresse angehängt: „/n“. In unserem Beispiel könnte die IP-Adresse also auch als „192.168.170.237/24“ geschrieben werden. Dieser Schreibweise ist zu entnehmen, dass die Netzmaske aus 24 Einsen gefolgt von 8 Nullen besteht.

Subnetzadressierung

Ein Blick auf die Adressstrukturen lässt erkennen, dass selbst bei Adressen der Klasse C eine große Anzahl von Hosts pro Netzwerk zulässig ist. Eine solche Struktur bedeutet eine ineffiziente Adressennutzung, wenn für jedes Ende einer Routerverbindung eine andere Netzwerkadresse erforderlich ist. Kleinere Büro-LANs verfügen häufig nicht über die dafür erforderliche Geräteanzahl. Die Lösung für dieses Problem heißt Subnetzadressierung.

Die Subnetzadressierung ermöglicht die Aufteilung einer IP-Netzwerkadresse in mehrere kleinere physikalische Netzwerke, die auch als Subnetze bezeichnet werden. Dabei werden einige der Hostadressen als Subnetznummern verwendet. Eine Adresse der Klasse B ergibt 16 Bit an Hostadressen bzw. 64.000 Hosts. Da die meisten Organisationen keine 64.000 Hosts benötigen, bleiben freie Bits übrig, die anders vergeben werden können. Mit Hilfe der Subnetzadressierung können diese freien Bits genutzt werden (vgl. Abbildung unten).

Abbildung B-2: Subnetz in einer Adresse der Klasse B

Eine Adresse der Klasse B kann auch in viele Adressen der Klasse C aufgeteilt werden. Ein Beispiel: Die IP-Adresse „172.16.0.0“ wurde vergeben, doch es gibt nicht mehr als 255 Hostadressen. Dadurch stehen 8 zusätzliche Bits für die Subnetzadresse zur Verfügung. Zur Verdeutlichung: Bei der IP-Adresse „172.16.97.235“ ist 172.16 die IP-Netzwerkadresse, 97 die Subnetzadresse und 235 die Hostadresse. Neben der Erweiterung der verfügbaren Adressen hat die Subnetzadressierung jedoch auch noch andere Vorteile. Mit Hilfe der Subnetzadressierung kann ein Netzwerkmanager ein Adressschema für das Netzwerk entwickeln, bei dem für die einzelnen geografischen Standorte oder Abteilungen der Organisation unterschiedliche Subnetze eingerichtet werden.

Auch wenn im obigen Beispiel das gesamte dritte Oktett für eine Subnetzadresse verwendet wird, ist die Einrichtung von Subnetzen keineswegs auf die Grenzen eines Oktetts beschränkt. Wenn Sie weitere Netzwerknummern benötigen, müssen Sie lediglich einige Bits von der Hostadresse in die Netzwerkadresse verschieben. Angenommen, Sie möchten eine Netzwerknummer der Klasse C (z. B. „192.68.135.0“) in zwei Nummern unterteilen. Dann verschieben Sie ein Bit von der Hostadresse in die Netzwerkadresse. Die neue Netzmaske (oder Subnetzmaske) lautet: 255.255.255.128. Das erste Subnetz hat die Netzwerknummer „192.68.135.0“ mit Hosts von „192.68.135.1“ bis „192.68.135.126“, das zweite Subnetz hat die Netzwerknummer „192.68.135.128“ mit Hosts von „192.68.135.129“ bis „192.68.135.254“.

Hinweis: Die Nummer „192.68.135.127“ wird nicht vergeben, da sie die Broadcast-Adresse des ersten Subnetzes ist. Die Nummer „192.68.135.128“ wird nicht vergeben, da sie die Netzwerk-Adresse des zweiten Subnetzes ist.

In der folgenden Tabelle sind die zusätzlichen Subnetzmaskenbits in Dezimalschreibweise aufgeführt. So verwenden Sie diese Tabelle: Schreiben Sie die ursprüngliche Netzmaske der Klasse auf und ersetzen Sie die Oktetts mit dem Wert „0“ durch den Wert der zusätzlichen Subnetz-Bits in Dezimalschreibweise. Wenn Sie zum Beispiel ein Netzwerk der Klasse C mit der Subnetzmaske „255.255.255.0“ in 16 Subnetze (4 Bit) unterteilen möchten, ist die neue Subnetzmaske „255.255.255.240“.

Tabelle B-1. Tabelle zur Netzmaskennotationsumwandlung für ein Oktett

Bits	Wert in Dezimalschreibweise
1	128
2	192
3	224
4	240
5	248
6	252
7	254
8	255

Die folgende Tabelle enthält eine Auswahl häufiger Netzmaskenwerte in Dezimalschreibweise und die Maskenlängenformate.

Tabelle B-2. Netzmaskenformate

Dezimalschreibweise	Maskenlänge
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30
255.255.255.254	/31
255.255.255.255	/32

Achten Sie bei der Konfiguration darauf, dass alle Hosts in einem LAN-Segment dieselbe Netzmaske verwenden. Dies empfiehlt sich aus folgenden Gründen:

- Nur so können alle Hosts lokale IP-Broadcast-Datenpakete erkennen.

  Wenn ein Gerät Broadcasts an seine Segmentnachbarn überträgt, verwendet es als Zieladresse die lokale Netzwerkadresse mit lauter Einsen als Hostadresse. Damit diese Vorgehensweise funktioniert, müssen auf allen Geräten im Segment dieselben Bits als Hostadresse konfiguriert sein.
- Nur so kann ein lokaler Router oder eine lokale Bridge erkennen, welche Adressen lokal und welche entfernt sind.

Private IP-Adressen

Wenn Ihr lokales Netzwerk vom Internet isoliert ist (z. B. wenn Sie NAT verwenden), können Sie den Hosts beliebige IP-Adressen zuweisen, ohne dass dadurch Probleme entstehen. Die folgenden drei Blöcke von IP-Adressen wurden jedoch von der IANA speziell für private Netzwerke reserviert:

```
10.0.0.0 bis 10.255.255.255
172.16.0.0 bis 172.31.255.255
192.168.1.0 bis 192.168.255.255
```

Wählen Sie Ihre private Netzwerknummer also am besten aus diesen Bereichen aus. Der DHCP-Server des WPN824 Routers ist so vorkonfiguriert, dass er automatisch private Adressen vergibt.

Erstellen Sie unter keinen Umständen beliebige IP-Adressen, sondern folgen Sie immer den Hinweisen hier. Weitere Informationen zur Adresszuweisung finden Sie in den Dokumenten RFC 1597, „*Address Allocation for Private Internets*“, und RFC 1466, „*Guidelines for Management of IP Address Space*“. Die RFCs sind auf der Website der Internet Engineering Task Force (IETF) unter www.ietf.org veröffentlicht.

Betrieb mit einer einzelnen IP-Adresse mit Hilfe von NAT

Um mehreren Computern eines LAN gleichzeitig den Zugriff aufs Internet zu ermöglichen, musste man lange Zeit mehrere IP-Adressen vom Internetdienstanbieter beziehen. Diese Art von Internetzugang ist teurer als ein Konto mit einer einzigen Adresse, wie es typischerweise von einem Einzelbenutzer mit einem Modem (statt eines Routers) eingesetzt wird. Der WPN824 Router verwendet zur gemeinsamen Nutzung von Adressen eine Methode namens NAT (Network Address Translation). Mit Hilfe dieser Methode können mehrere vernetzte Computer ein Internetkonto mit einer einzigen IP-Adresse gemeinsam nutzen. Die IP-Adresse kann dabei vom Internetdienstanbieter statisch oder dynamisch vergeben werden.

Diese gemeinsame Nutzung der Adresse wird dadurch ermöglicht, dass der Router die internen LAN-IP-Adressen in eine einzige Adresse umwandelt, die im Internet weltweit eindeutig ist. Die internen LAN-IP-Adressen können dabei entweder private oder registrierte Adressen sein. Weitere Informationen zur Umwandlung von IP-Adressen finden Sie im Dokument RFC 1631, „*The IP Network Address Translator (NAT)*“.

Die folgende Abbildung illustriert den Betrieb mit einer einzigen IP-Adresse.

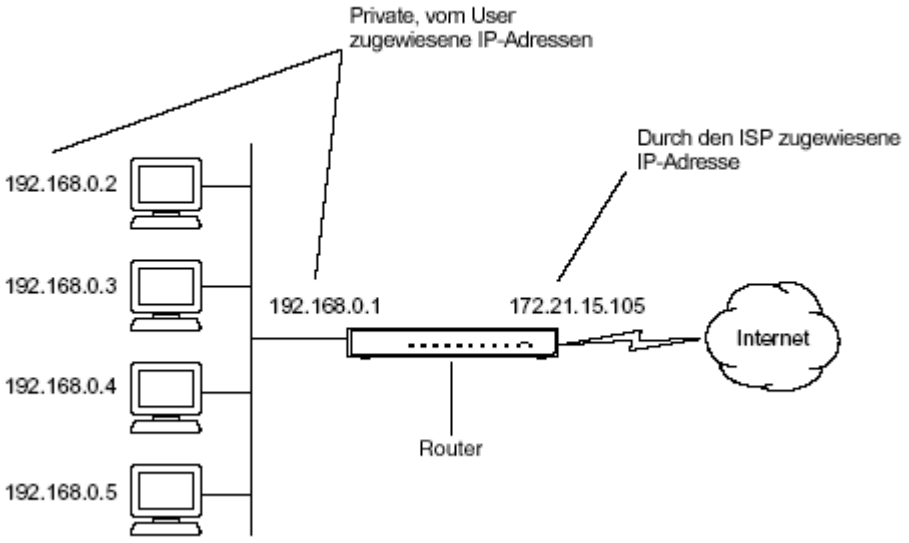


Abbildung B-3: Betrieb mit einer einzelnen IP-Adresse mit Hilfe von NAT

Die abgebildete Lösung bietet zudem einen Firewall-ähnlichen Schutz, da die internen LAN-Adressen im Internet auf Grund der Umwandlung bei der Verbindung nicht zu erkennen sind. Alle eingehenden Anforderungen werden durch den Router gefiltert. Diese Filterung kann verhindern, dass unbefugte Eindringlinge Ihr System ausspionieren. Mit Hilfe einer Portweiterleitung können Sie aber dennoch einen Computer in Ihrem lokalen Netzwerk (z. B. einen Webserver) für externe Benutzer zugänglich machen.

MAC-Adressen und ARP (Address Resolution Protocol)

Eine IP-Adresse allein reicht nicht aus, um Daten von einem LAN-Gerät an ein anderes zu senden. Um den Versand von Daten zwischen LAN-Geräten zu ermöglichen, muss die IP-Adresse des Zielgeräts in dessen MAC-Adresse (Media Access Control) umgewandelt werden. Jedes Gerät in einem Netzwerk verfügt über eine eindeutige MAC-Adresse. Bei der MAC-Adresse handelt es sich um eine 48-Bit-Nummer, die jedem Gerät vom Hersteller zugewiesen wird. Zur Zuordnung von IP-Adressen zu MAC-Adressen wird ein Protokoll namens ARP (Address Resolution Protocol) verwendet. IP verwendet ARP zum Ermitteln von MAC-Adressen.

Wenn ein Gerät Daten an eine andere Station im Netzwerk sendet und die MAC-Zieladresse noch nicht erfasst ist, wird ARP verwendet. Dazu wird eine ARP-Anforderung an das Netzwerk gesendet. Alle Stationen des Netzwerks empfangen und lesen diese Anforderung. Die IP-Zieladresse der gewünschten Station ist in dieser Anforderung enthalten. So antwortet nur die Station mit dieser IP-Adresse auf die ARP-Anforderung. Alle anderen Stationen ignorieren die Anfrage.

Weiterführende Dokumente

Die Station mit der richtigen IP-Adresse antwortet mit ihrer eigenen MAC-Adresse direkt an das sendende Gerät. Die Empfängerstation gibt die gewünschte MAC-Zieladresse an die übertragende Station weiter. Die IP- und MAC-Adressdaten für die einzelnen Stationen werden in einer ARP-Tabelle gespeichert. Beim nächsten Versand von Daten kann die Adresse den in der Tabelle gespeicherten Informationen entnommen werden.

Weitere Informationen zur Adresszuweisung finden Sie in den IETF-Dokumenten RFC 1597, „*Address Allocation for Private Internets*“, und RFC 1466, „*Guidelines for Management of IP Address Space*“.

Weitere Informationen zur Umwandlung von IP-Adressen finden Sie im Dokument RFC 1631, „*The IP Network Address Translator (NAT)*“.

DNS-Server

Viele der Ressourcen im Internet können über einfache beschreibende Namen wie *www.NETGEAR.com* erreicht werden. Diese Art der Adressierung ist auf der Anwendungsebene sehr praktisch, doch damit ein Benutzer wirklich auf die Ressource zugreifen kann, muss der beschreibende Name in eine IP-Adresse umgewandelt werden. Ähnlich wie ein Telefonbuch bestimmten Namen bestimmte Telefonnummern zuordnet oder eine ARP-Tabelle IP-Adressen die entsprechenden MAC-Adressen zuordnet, ordnet ein DNS-Server (Domain Name System) beschreibenden Namen die richtigen IP-Adressen zu.

Wenn ein Computer über einen beschreibenden Namen auf eine Ressource zugreift, kontaktiert er dabei zuerst einen DNS-Server, um die IP-Adresse der Ressource zu erfahren. Der Computer sendet die gewünschte Nachricht über die IP-Adresse. Viele große Unternehmen, wie z. B. Internetdienstanbieter, haben eigene DNS-Server und gestatten ihren Kunden die Benutzung dieser Server zum Nachschlagen von Adressen.

IP-Konfiguration über DHCP

Bei der Installation eines IP-basierten LANs muss für jeden Computer eine IP-Adresse konfiguriert werden. Wenn der Computer auf das Internet zugreifen soll, sollten zudem eine Gateway-Adresse und eine oder mehrere DNS-Serveradressen konfiguriert werden. Als Alternative zur manuellen Konfiguration gibt es auch eine Methode, mit der jeder Computer im Netzwerk diese Konfigurationsdaten automatisch abrufen kann: Ein Gerät im Netzwerk wird als DHCP-Server (Dynamic Host Configuration Protocol) eingesetzt. Der DHCP-Server speichert neben anderen Informationen (darunter Gateway- und DNS-Adressen) eine Liste von IP-Adressen, die er an andere Geräte im Netzwerk vergeben kann. Der WPN824 Router kann als DHCP-Server eingesetzt werden.

Beim Verbindungsaufbau zum Internetdienstarbeiter dient der WPN824 Router außerdem als DHCP-Client. Falls der Internetdienstanbieter diese Informationen per DHCP zur Verfügung stellt, kann die Firewall automatisch IP-Adresse, Subnetzmaske, DNS-Serveradressen und eine Gateway-Adresse abrufen.

Internetsicherheit und Firewalls

Wenn Ihr LAN über einen Router an das Internet angeschlossen ist, besteht die Gefahr, dass Eindringlinge von außen auf Ihr Netzwerk zugreifen oder Störungen verursachen. Ein NAT-Router gewährt hier einen gewissen Schutz, da bei diesem Verfahren das Netzwerk hinter dem Router vor externen Zugriffen über das Internet geschützt ist. Hartnäckige Hacker können sich allerdings dennoch Informationen über Ihr Netzwerk verschaffen oder zumindest Ihre Internetverbindung unterbrechen. Besseren Schutz bietet ein Firewall-Router.

Was ist eine Firewall?

Eine Firewall ist ein Gerät, das ein Netzwerk vor einem anderen Netzwerk schützt, aber dennoch einen Austausch zwischen den beiden Netzwerken zulässt. Eine Firewall beinhaltet die Funktionen eines NAT-Routers, ergänzt diese jedoch um weitere Funktionen zur Abwehr von unbefugten Zugriffen und Angriffen durch Hacker. Eine Reihe bekannter Typen von Zugriffsversuchen und Hackerangriffen kann erkannt werden, sobald sie auftreten. Wenn es zu einem Vorfall kommt, kann die Firewall Einzelheiten des Angriffsversuchs protokollieren und ggf. den Administrator per E-Mail benachrichtigen. Mit den im Protokoll festgehaltenen Daten kann der Administrator sich dann an den Internetdienstanbieter des Hackers wenden. Bei manchen Arten von Zugriffsversuch kann die Firewall den Hacker abwehren, indem alle weiteren Pakete, die von der IP-Adresse des Hackers stammen, für eine gewisse Zeit ignoriert werden.

SPI (Stateful Packet Inspection)

Anders als gewöhnliche Router für die gemeinsame Internetnutzung verwendet eine Firewall einen Prozess namens SPI (Stateful Packet Inspection). Dabei wird das Netzwerk durch sichere Firewall-Filterung vor Angriffen und Zugriffsversuchen geschützt. Da Benutzeranwendungen wie FTP und Webbrowser komplexe Netzwerkverkehrsmuster schaffen können, muss die Firewall in der Lage sein, den Status von Netzwerkverbindungen gruppenweise zu analysieren. Durch SPI werden eingehende Pakete in der Vermittlungsschicht abgefangen und dann in Bezug auf statusbezogene Informationen zu allen Netzwerkverbindungen analysiert. Ein zentraler Cache-Speicher innerhalb der Firewall protokolliert die Statusinformationen zu allen Netzwerkverbindungen. Der gesamte Datenverkehr, der durch die Firewall geht, wird in Hinblick auf den Status dieser Verbindung analysiert. Dadurch wird bestimmt, ob die Daten durchgelassen oder abgelehnt werden.

Denial-of-Service-Angriffe

Mit Denial-of-Service-Angriffen (DoS) können Hacker Ihr Netzwerk funktionsunfähig machen oder die Kommunikation verhindern. Ein derartiger Angriff kann mit ganz einfachen Mitteln geschehen. Es reicht schon aus, Ihre Website mit mehr Anfragen zu überschwemmen, als diese verarbeiten kann. Ein etwas raffinierterer Angreifer versucht vielleicht, Schwachstellen im Betriebssystem Ihres Routers oder Gateways auszunutzen. Manche Betriebssysteme können z. B. schon durch Senden eines Datenpakets mit falschen Längenangaben gestört werden.

Netzwerk-Verkabelung

Ursprünglich wurden für Netzwerke dicke oder dünne Koaxialkabel verwendet, doch inzwischen werden meistens ungeschirmte Twisted-Pair-Kabel (UTP) eingesetzt. Ein UTP-Kabel besteht aus vier miteinander verdrillten Aderpaaren und hat einen RJ45-Stecker. Ein normales UTP-Patchkabel (Durchgangskabel) entspricht der Standardverdrahtung nach EIA568B, die unten in Tabelle B-3 dargestellt ist.

Tabelle B-3. Verdrahtung eines UTP-Patchkabels

Pin	Leitungsfarbe	Signal
1	Orange/Weiß	Senden (Tx) +
2	Orange	Senden (Tx) -
3	Grün/Weiß	Empfangen (Rx) +
4	Blau	
5	Blau/Weiß	
6	Grün	Empfangen (Rx) -
7	Braun/Weiß	
8	Braun	

Kabel der Kategorie 5

Kabel der Kategorie 5 (CAT 5), die den Standards ANSI/EIA/TIA-568-A entsprechen, dürfen eine Gesamtlänge von 100 m nicht überschreiten. Diese Länge ist wie folgt aufzuteilen:

6 m zwischen dem Switch und dem Patch-Panel (falls eines verwendet wird)

90 m zwischen dem Kabelschrank und der Wandsteckdose

3 m zwischen der Wandsteckdose und dem Desktop-Gerät

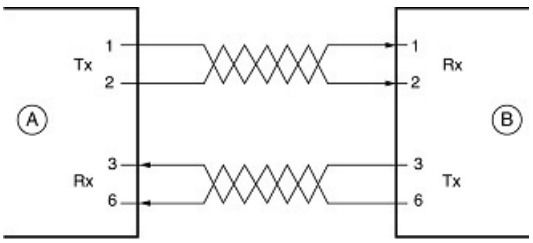
Das Patch-Panel und sonstige Geräte müssen den Anforderungen für den Betrieb bei 100 MBit/s (Kategorie 5) entsprechen. An den Schnittstellen darf das Leitungspaar jeweils max. 1,5 cm entdrillt werden.

Bei Twisted-Pair-Netzwerken, die mit 10 MBit/s (10BASE-T) arbeiten, wirkt es sich meist nicht nachteilig aus, wenn Kabel von niedriger Qualität verwendet werden. Bei 100 MBit/s (100BASE-Tx) muss das Kabel dagegen der Kategorie 5 (Cat 5) der EIA (Electronic Industries Alliance) entsprechen. Diese Kategorie ist auf die Kabelummantelung aufgedruckt. Ein Kabel der Kategorie 5 erfüllt besondere Anforderungen hinsichtlich Datenverlust und Störsignalen. Sowohl bei Netzwerken mit 10 MBit/s als auch bei Netzwerken mit 100 MBit/s sind zudem Einschränkungen bezüglich der maximalen Kabellänge zu berücksichtigen.

Das Innenleben eines Twisted-Pair-Kabels

Damit zwei Geräte miteinander kommunizieren können, muss der Sender jedes Geräts mit dem Empfänger des jeweils anderen Geräts verbunden sein. Die Crossover-Funktion ist normalerweise in die Schaltkreise des Geräts integriert. Adapterkarten für Computer und Workstations sind in der Regel MDI-Ports (Media Dependent Interface), die auch als Uplink-Ports bezeichnet werden. Die meisten Repeater und Switch-Ports sind als MDI mit integrierten Crossover-Ports konfiguriert. Diese werden als MDI-X-Ports oder normale Ports bezeichnet. Die Auto Uplink-Technologie erkennt automatisch, welche Verbindungsart (MDI oder MDI-X) benötigt wird, und stellt die richtige Verbindung her.

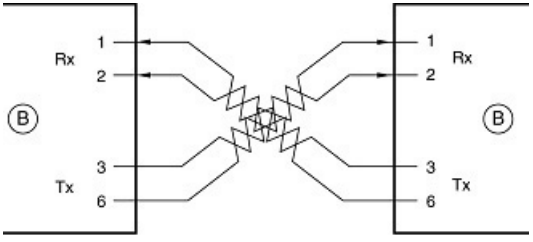
Abbildung B-4 zeigt ein Twisted-Pair-Durchgangskabel



A = Uplink- oder MDI-Port (z. B. an einem PC)
B = Normal- oder MDI-X-Port (z. B. an einem Switch)
1, 2, 3, 6 = Pinnummern

Abbildung B-4: Twisted-Pair-Durchgangskabel

Abbildung B-5 zeigt ein Twisted-Pair-Crossover-Kabel



B = Normal- oder MDI-X-Port (z. B. an einem Switch)
1, 2, 3, 6 = Pinnummern

Abbildung B-5: Twisted-Pair-Crossover-Kabel

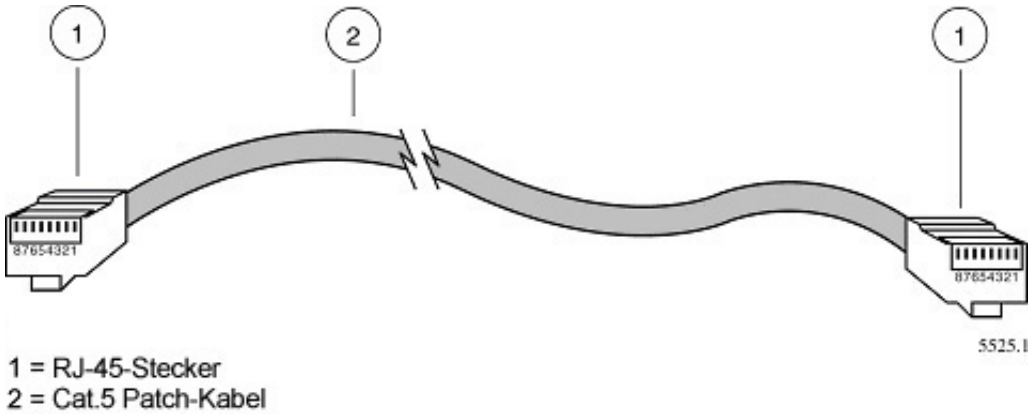


Abbildung B-6: UTP-Kabel der Kategorie 5 mit RJ-45-Stecker an beiden Enden

Hinweis: Manche Telefonkabel können auch über einen RJ-45-Stecker verfügen. Die Verwendung von Telefonkabeln führt jedoch zu einer Vielzahl von Kollisionen, so dass der darüber angeschlossene Port partitioniert oder vom Netzwerk getrennt wird.

Uplink-Switches, Crossover-Kabel und MDI-/MDIX-Umschaltung

In der Verdrahtungstabelle weiter oben sind die Signale „Senden“ und „Empfangen“ aus der Perspektive des Computers dargestellt, der als MDI (Media Dependent Interface) verdrahtet ist. Bei dieser Verdrahtung sendet der Computer über die Pins 1 und 2. Im Switch wird die Perspektive umgekehrt, und über die Pins 1 und 2 erfolgt der Empfang. Diese Art der Verdrahtung wird als „MDI-X“ (Media Dependant Interface - Crossover) bezeichnet.

Wenn ein Computer mit einem anderen Computer oder ein Switch-Port mit einem anderen Switch-Port verbunden werden soll, muss das Senderpaar mit dem Empfängerpaar vertauscht werden. Dieser Tausch kann über einen der folgenden zwei Mechanismen bewerkstelligt werden. Die meisten Switches verfügen über einen Uplink-Umschalter, der es ermöglicht, die Paare an einem Port zu vertauschen, so dass dieser Port über ein normales Netzwerkkabel mit einem anderen Switch verbunden werden kann. Die zweite Möglichkeit ist die Verwendung eines Crossover-Kabels. Dabei handelt es sich um ein spezielles Kabel, bei dem das Sender- und Empfängerpaar in einem der Anschlüsse vertauscht ist. Crossover-Kabel sind oft nicht als solche gekennzeichnet, können jedoch durch einen Vergleich der beiden Anschlüsse identifiziert werden. Da die Stecker aus durchsichtigem Plastik sind, kann man sie leicht nebeneinander legen und die Reihenfolge der Leitungsfarben vergleichen. Bei einem Durchgangskabel ist die Farbreihenfolge in beiden Steckern gleich. Bei einem Crossover-Kabel sind das orangefarbene und das grüne Paar bei einem der beiden Stecker vertauscht.

Der WPN824 Router verwendet die Auto Uplink™-Technologie (auch als MDI/MDIX bezeichnet). Dies bedeutet, dass jeder LAN-Port automatisch erkennt, ob für das eingesteckte Netzwerkkabel eine normale Verbindung (d. h. eine Verbindung zu einem Computer) oder eine Uplink-Verbindung (d. h. eine Verbindung zu einem Router oder Switch) erforderlich ist. Der Port konfiguriert sich dann den Anforderungen entsprechend selbst. Diese Funktion macht zudem die Verwendung von Crossover-Kabeln unproblematisch, da Auto Uplink™ bei beiden Kabeltypen die richtige Verbindung herstellt.

Anhang C
Netzwerkeinrichtung

In diesem Anhang wird beschrieben, wie Sie Ihr Netzwerk auf eine Internetverbindung über den RangeMax Wireless Router WPN824 vorbereiten und überprüfen, ob der Breitband-Internetservice Ihres Internetdienstanbieters (kurz ISP) bereit ist.

	Hinweis: Wenn ein Techniker Ihres Internetdienstanbieters Ihren Computer bei der Installation eines Breitbandmodems konfiguriert hat oder wenn Sie ihn nach Anleitung Ihres Dienstanbieters konfiguriert haben, sollten Sie die aktuellen Konfigurationsdaten für die Konfiguration Ihrer Firewall übernehmen. Notieren Sie sich diese Informationen, bevor Sie Ihre Computer neu konfigurieren. Weitere Informationen dazu finden Sie unter „Ermitteln der ISP-Konfigurationsdaten für Windows-Computer“ auf Seite C-21 oder „Ermitteln der ISP-Konfigurationsdaten für Apple-Computer“ auf Seite C-22.

Voraussetzungen zum Einsatz eines Routers mit einem Breitbandmodem

Vor Beginn müssen Sie folgende Vorbereitungen treffen:

Kabel und Computer-Hardware

Der WPN824 Router kann in Ihrem Netzwerk nur eingesetzt werden, wenn jeder Computer mit einem 802.11g- oder 802.11b-Wireless-Adapter bzw. einer kabelgebundenen Netzwerkkarte und einem Netzwerkkabel ausgestattet ist. Wenn Ihr Computer die Verbindung zum Netzwerk über eine Netzwerkkarte mit 100 MBit/s herstellt, müssen Sie ein CAT-5-Kabel (Kategorie 5) wie das im Lieferumfang Ihres Routers enthaltene verwenden. Erläuterungen zur Verkabelung finden Sie unter „Netzwerk-Verkabelung“ auf Seite B-11. Das Kabel- oder DSL-Breitbandmodem muss über eine übliche 10 MBit/s Ethernet-Schnittstelle (10BASE-T) oder über eine 100 MBit/s Fast Ethernet-Schnittstelle (100BASE-Tx) verfügen.

Netzwerkkonfiguration des Computers

Der WPN824 wird mit einer integrierten Konfigurationsoberfläche (Web Configuration Manager) geliefert. Für den Zugriff auf die Konfigurationsmenüs des WPN824 muss auf Ihrem Computer ein Java-fähiger Webbrowser, der HTTP-Uploads unterstützt, installiert sein (z. B. Microsoft Internet Explorer oder Netscape Navigator). Verwenden Sie Internet Explorer bzw. Netscape Navigator 4.0 oder höher.

Für die erste Konfiguration Ihres Routers müssen Sie einen Computer über ein Netzwerkkabel an den Router anschließen. Dieser Computer muss so eingerichtet sein, dass er seine TCP/IP-Konfiguration vom Router automatisch über DHCP erhält.

Hinweis: Hilfe zur DHCP-Konfiguration erhalten Sie in den Lehrgängen zur TCP/IP-Konfiguration unter Windows auf der *Ressourcen-CD für den NETGEAR RangeMax Wireless Router WPN824* oder in diesem Anhang.

Konfiguration des Internetzugangs

Je nachdem, wie der Internetzugang von Ihrem Internetdienstanbieter eingerichtet wurde, benötigen Sie einen oder mehrere der folgenden Konfigurationsparameter zum Anschluss des Routers an das Internet:

- Host- und Domainnamen
- Benutzernamen und Passwort zur Anmeldung beim Internetdienstanbieter
- DNS-Serveradressen (Domain Name Server) des Internetdienstanbieters
- Feste IP-Adresse, auch statische IP-Adresse genannt

Wo erhalte ich die Parameter für die Internetkonfiguration?

Die erforderlichen Informationen für die Internetverbindung können Sie auf unterschiedliche Weise erhalten.

- Ihr Internetdienstanbieter liefert alle Informationen, die Sie für die Verbindung zum Internet benötigen. Wenn Sie diese Informationen nicht finden können, fordern Sie sie bei Ihrem Internetdienstanbieter an oder versuchen Sie es mit einer der unten genannten Möglichkeiten.
- Wenn Sie einen Computer mit einer bestehenden Internetverbindung haben, können Sie die Informationen auf diesem Computer abrufen.
  - — Öffnen Sie unter Windows 95/98/ME die Systemsteuerung, wählen Sie unter „Netzwerk“ den TCP/IP-Eintrag für den Netzwerk-Adapter und klicken Sie auf **Eigenschaften**. Notieren Sie die Einstellungen, die auf jeder Registerkarte stehen.
  - — Öffnen Sie unter Windows 2000/XP die LAN-Verbindung, wählen Sie den TCP/IP-Eintrag für den Netzwerk-Adapter und klicken Sie auf **Eigenschaften**. Notieren Sie die Einstellungen, die auf jeder Registerkarte stehen.
  - — Notieren Sie bei Apple-Computern die Einstellungen im TCP/IP- oder Netzwerk-Kontrollfeld.
- Sie können auch in der ISP-Anleitung für NETGEAR-Router auf der *Ressourcen-CD für den NETGEAR RangeMax Wireless Router WPN824* nachschlagen. Dort sind Verbindungsinformationen für viele Internetdienstanbieter aufgeführt.

Wenn Sie die Parameter für Ihre Internetkonfiguration gefunden haben, können Sie sie auf der nächsten Seite notieren.

Aufzeichnung der Internetzugangsdaten

Drucken Sie diese Seite aus. Tragen Sie die Konfigurationsparameter Ihres Internetdienstanbieters (ISP) ein.

ISP-Benutzername: Bei der Eingabe des Benutzernamens und Passworts für die Anmeldung kommt es auf die genaue Schreibweise (mit Groß- und Kleinschreibung) an, die Sie von Ihrem Internetdienstanbieter erhalten haben. Manche Internetdienstanbieter verwenden Ihre vollständige E-Mail-Adresse als Benutzernamen. Der Dienstname wird nicht von allen Internetdienstanbietern gefordert. Wenn Sie sich mit einem Benutzernamen und Passwort anmelden, tragen Sie Folgendes ein:

Benutzername: _____

Passwort: _____

Dienstname: _____

Feste oder statische IP-Adresse: Wenn Sie eine statische IP-Adresse haben, notieren Sie die folgenden Informationen. 169.254.141.148 ist ein Beispiel für eine gültige IP-Adresse.

Feste oder statische Internet-IP-Adresse: _____ _____ _____ _____

Gateway-IP-Adresse: _____ _____ _____ _____

Subnetzmaske: _____ _____ _____ _____

DNS-Serveradressen des Internetdienstanbieters: Wenn Sie DNS-Serveradressen erhalten haben, tragen Sie Folgendes ein:

Erste DNS-Server-IP-Adresse: _____ _____ _____ _____

Zweite DNS-Server-IP-Adresse: _____ _____ _____ _____

Host- und Domainnamen: Manche Internetdienstanbieter verwenden einen bestimmten Host- oder Domainnamen, z. B. **CCA7324-A** oder **home**. Wenn Sie keine Host- oder Domainnamen erhalten haben, können Sie sich von den folgenden Beispielen anregen lassen:

- Wenn Ihr vorrangiges E-Mail-Konto bei Ihrem Internetdienstanbieter **aaa@yyy.de** lautet, verwenden Sie **aaa** als Hostnamen. Ihr Internetdienstanbieter kann ihn als Konto-, Benutzer-, Host-, Computer- oder Systemnamen bezeichnen.
- Wenn der Mailserver Ihres Internetdienstanbieters **mail.xxx.yyy.de** heißt, verwenden Sie **xxx.yyy.de** als Domainnamen.

Hostname des ISP: _____ Domainname des ISP: _____

Drahtloser Zugriff: Lesen Sie das Arbeitsblatt zur Konfiguration unter „Erforderliche Information vor der Änderung grundlegender WLAN-Einstellungen“ auf Seite 4-7.

Einrichten der Computer für den TCP/IP-Netzwerkbetrieb

Computer greifen über ein Protokoll namens TCP/IP (Transmission Control Protocol/Internet Protocol) auf das Internet zu. Auf jedem Computer in Ihrem Netzwerk muss TCP/IP installiert und als Netzwerkprotokoll ausgewählt sein. Wenn in Ihrem Computer bereits eine Netzwerkkarte installiert ist, ist TCP/IP vermutlich ebenfalls installiert.

Die meisten Betriebssysteme schließen die für den Netzwerkbetrieb über TCP/IP erforderlichen Softwarekomponenten ein:

- Windows® 95 oder spätere Versionen enthalten die Softwarekomponenten zur Einrichtung eines TCP/IP-Netzwerks.
- Windows 3.1 enthält keine TCP/IP-Komponente. Sie müssen ein TCP/IP-Anwendungspaket eines Drittanbieters, wie NetManage Chameleon, erwerben.
- Das Betriebssystem Mac OS 7 oder spätere Versionen enthalten die Softwarekomponenten zur Einrichtung eines TCP/IP-Netzwerks.
- Alle Versionen von UNIX oder Linux enthalten TCP/IP-Komponenten. Befolgen Sie die Anleitungen für Ihr Betriebssystem oder Ihre Netzwerksoftware, um TCP/IP auf Ihrem Computer zu installieren.

In Ihrem IP-Netzwerk müssen alle Computer und die Firewall eine eindeutige IP-Adresse erhalten. Außerdem benötigt jeder Computer bestimmte andere IP-Konfigurationsdaten, wie Subnetzmaske (Teilnetzmaske), DNS-Adresse (Domain Name Server) und Standardgateway-Adresse. In den meisten Fällen sollten Sie TCP/IP so installieren, dass der Computer die jeweiligen Informationen zur Netzwerkkonfiguration automatisch während des Systemstarts von einem DHCP-Server abruft. Eine ausführliche Erläuterung der Bedeutung und des Zwecks dieser Konfigurationsdaten finden Sie in Anhang B, „Netzwerke, Routing, Firewalls und Grundlagen“.

Der WPN824 Router ist im Auslieferungszustand bereits als DHCP-Server vorkonfiguriert. Beim erneuten Systemstart der PCs legt die Firewall automatisch die folgenden Informationen zur TCP/IP-Konfiguration fest:

- IP-Adressen für PCs oder Workstations: 192.168.1.2 bis 192.168.1.254
- Subnetzmaske: 255.255.255.0
- Gateway-Adresse (die Firewall): 192.168.1.1

Diese Adressen gehören zum Bereich der von der IETF (Internet Engineering Task Force) festgelegten privaten Adressen, die für private Netzwerke reserviert sind.

Einrichten von Windows 95, 98 und Me für den TCP/IP-Netzwerkbetrieb

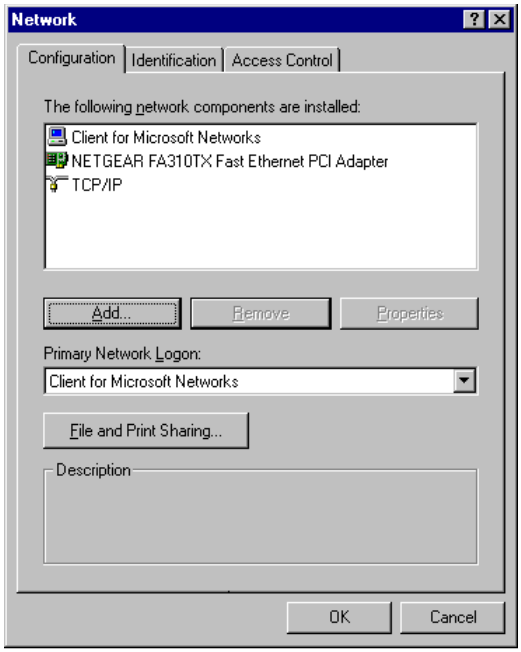
Im Rahmen der PC-Einrichtung müssen Sie manuell auf jedem PC im Netzwerk TCP/IP installieren und konfigurieren. Halten Sie dazu Ihre Windows-CD bereit; sie wird möglicherweise bei der TCP/IP-Installation benötigt.

Installieren oder Überprüfen der Windows-Netzwerkkomponenten

So installieren oder überprüfen Sie die erforderlichen Komponenten für den IP-Netzwerkbetrieb:

1. Klicken Sie in der Windows-Taskleiste auf die Schaltfläche **Start**, wählen Sie **Einstellungen** und klicken Sie dann auf **Systemsteuerung**.
2. Doppelklicken Sie auf das Symbol **Netzwerk**.

   Daraufhin wird das Fenster „Netzwerk“ (Network) mit einer Liste der installierten Komponenten geöffnet:



   Sie benötigen einen Netzwerk-Adapter, das TCP/IP-Protokoll und den „Client für Microsoft-Netzwerke“ (Client for Microsoft Networks).

	Hinweis: Die anderen im Fenster „Netzwerk“ angezeigten Netzwerkkomponenten brauchen nicht vor der Installation des Adapters, von TCP/IP oder dem „Client für Microsoft-Netzwerke“ entfernt zu werden.

Zum Installieren eines neuen Adapters gehen Sie wie folgt vor:

a. Klicken Sie auf die Schaltfläche **Hinzufügen** (Add).

b. Wählen Sie **Adapter** und klicken Sie dann auf **Hinzufügen**.

c. Wählen Sie den Hersteller und das Modell Ihres Netzwerk-Adapters und klicken Sie dann auf **OK**.

Zum Installieren von TCP/IP gehen Sie wie folgt vor:

a. Klicken Sie auf die Schaltfläche **Hinzufügen**.

b. Wählen Sie **Protokoll** und klicken Sie dann auf **Hinzufügen**.

c. Wählen Sie **Microsoft**.

d. Wählen Sie **TCP/IP** und klicken Sie dann auf **OK**.

Zum Installieren des „Client für Microsoft-Netzwerke“ gehen Sie wie folgt vor:

a. Klicken Sie auf die Schaltfläche **Hinzufügen**.

b. Wählen Sie **Client** und klicken Sie dann auf **Hinzufügen**.

c. Wählen Sie **Microsoft**.

d. Wählen Sie **Client für Microsoft-Netzwerke** und klicken Sie dann auf **OK**.

3. Starten Sie den PC neu, damit die Änderungen in Kraft treten.

Einrichten von DHCP zur automatischen Konfiguration von TCP/IP-Einstellungen unter Windows 95B, 98 und Me

Wenn die Komponenten für das TCP/IP-Protokoll installiert sind, müssen jedem PC spezifische Informationen über den PC und die in seinem Netzwerk verfügbaren Ressourcen zugewiesen werden. Diese Informationen lassen sich am einfachsten konfigurieren, wenn Sie den PC anweisen, die Informationen von einem DHCP-Server im Netzwerk abzurufen.

Sie werden feststellen, dass sich die Verfahren bei der Verwendung von DHCP zur Konfiguration von TCP/IP in den verschiedenen Windows-Systemen ähnlich sind.

Die folgenden Schritte führen Sie durch den Konfigurationsvorgang für jede dieser Windows-Versionen.

1

Suchen Sie das Symbol **Netzwerkumgebung**.

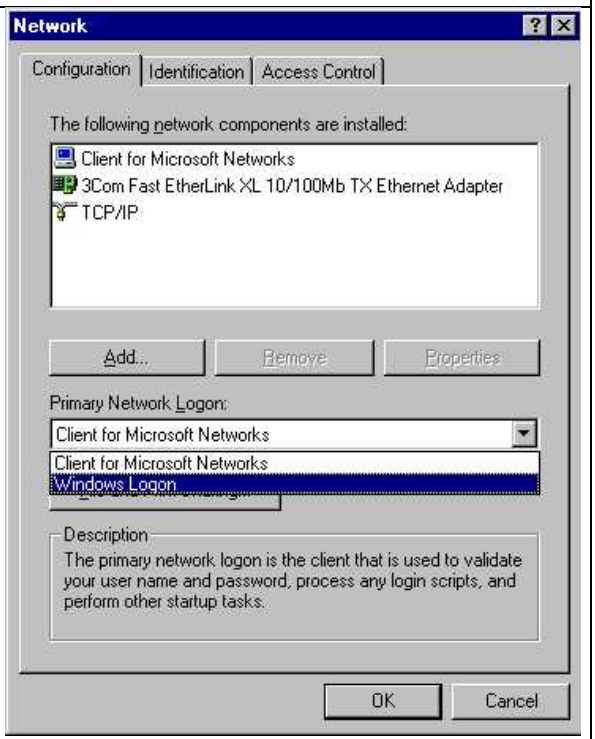
- Wenn sich dieses Symbol auf dem Windows-Desktop befindet, zeigen Sie mit der Maus darauf und drücken Sie die rechte Maustaste.
- Wenn sich das Symbol nicht auf dem Desktop befindet:
  - Klicken Sie in der Taskleiste unten links im Fenster auf **Start**.
  - Wählen Sie **Einstellungen** und dann **Systemsteuerung**.
  - Suchen Sie das Symbol **Netzwerkumgebung** und klicken Sie darauf. Damit öffnen Sie das unten gezeigte Fenster „Netzwerk“ (Network).

2

Überprüfen Sie die folgenden Einstellungen, wie in der Abbildung zu sehen:

- „Client für Microsoft-Netzwerke“ (Client for Microsoft Networks) ist vorhanden
- Netzwerk-Adapter ist vorhanden
- TCP/IP ist vorhanden
- **Primäre Netzwerkanmeldung** (Primary Network Logon) ist auf „Windows-Anmeldung“ (Windows Logon) eingestellt

Klicken Sie auf die Schaltfläche **Eigenschaften** (Properties). Daraufhin wird das folgende Fenster mit den TCP/IP-Eigenschaften (TCP/IP Properties) angezeigt.



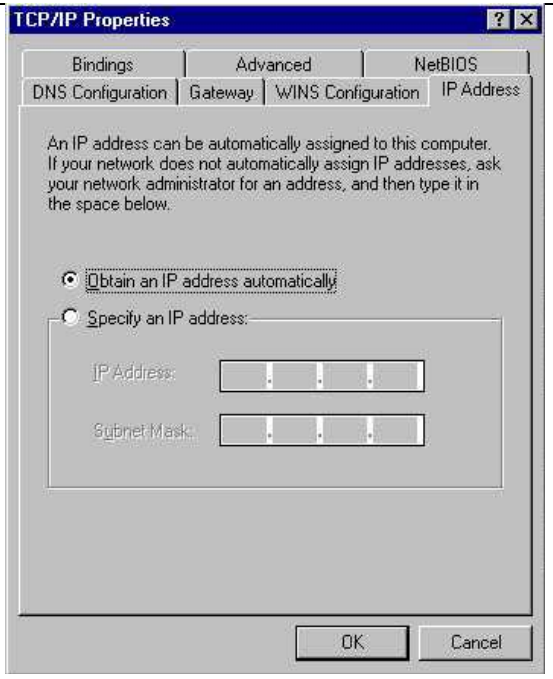
3

- Standardmäßig ist in diesem Fenster die Registerkarte „IP-Adresse“ (IP Address) geöffnet.
- Überprüfen Sie Folgendes:

  IP-Adresse automatisch beziehen (Obtain an IP address automatically) ist ausgewählt. Falls die Option nicht ausgewählt ist, klicken Sie auf die Optionsschaltfläche links daneben, um sie zu aktivieren. Diese Einstellung ist erforderlich, damit der DHCP-Server automatisch eine IP-Adresse zuweisen kann.
- Klicken Sie zum Fortfahren auf **OK**.

Starten Sie den PC neu.

Wiederholen Sie diese Schritte auf jedem PC im Netzwerk, der diese Windows-Version verwendet.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

Auswählen der Internetzugriffsmethode unter Windows

1. Klicken Sie in der Windows-Taskleiste auf die Schaltfläche **Start**, wählen Sie **Einstellungen** und klicken Sie dann auf **Systemsteuerung**.
2. Doppelklicken Sie auf das Symbol **Internetoptionen**.
3. Wählen Sie **Internetverbindung manuell einrichten** oder **Internetverbindung über ein lokales Netzwerk (LAN) herstellen** und klicken Sie auf **Weiter**.
4. Wählen Sie **Internetverbindung über ein lokales Netzwerk (LAN) herstellen** und klicken Sie auf **Weiter**.
5. Deaktivieren Sie alle Kästchen auf dem Bildschirm für die LAN-Internetkonfiguration und klicken Sie auf **Weiter**.
6. Schließen Sie den Assistenten ab.

Überprüfen der TCP/IP-Eigenschaften

Nachdem Sie den PC konfiguriert und neu gestartet haben, können Sie die TCP/IP-Konfiguration mit dem Dienstprogramm *winipcfg.exe* überprüfen:

1. Klicken Sie in der Windows-Taskleiste auf die Schaltfläche **Start** und klicken Sie dann auf **Ausführen**.

2. Geben Sie den Befehl **`winipcfg`** ein und klicken Sie dann auf **OK**.

   Daraufhin wird das Fenster „IP-Konfiguration“ geöffnet, in dem u. a. Ihre IP-Adresse, Subnetzmaske und Standardgateway-Adresse aufgeführt sind.

3. Wählen Sie Ihren Netzwerk-Adapter aus der Dropdown-Liste aus.

   Das Fenster wird aktualisiert, um Ihre Einstellungen anzuzeigen; sie sollten mit den unten aufgeführten Werten übereinstimmen, wenn Sie die Standard-TCP/IP-Einstellungen verwenden, die NETGEAR für eine Verbindung über einen Router oder ein Gateway empfiehlt:

   - Die IP-Adresse liegt zwischen 192.168.1.2 und 192.168.1.254.
   - Die Subnetzmaske lautet 255.255.255.0.
   - Die Standardgateway-Adresse lautet 192.168.1.1.

Einrichten von Windows NT4, 2000 oder XP für den IP-Netzwerkbetrieb

Im Rahmen der PC-Einrichtung müssen Sie auf jedem PC im Netzwerk TCP/IP installieren und konfigurieren. Halten Sie dazu Ihre Windows-CD bereit; sie wird möglicherweise bei der TCP/IP-Installation benötigt.

Installieren oder Überprüfen der Windows-Netzwerkkomponenten

So installieren oder überprüfen Sie die erforderlichen Komponenten für den IP-Netzwerkbetrieb:

1. Klicken Sie in der Windows-Taskleiste auf die Schaltfläche **Start**, wählen Sie **Einstellungen** und klicken Sie dann auf **Systemsteuerung**.
2. Doppelklicken Sie auf das Symbol **Netzwerk- und DFÜ-Verbindungen**.
3. Wenn Ihr PC über einen Netzwerk-Adapter verfügt, sollten Sie einen Eintrag für „LAN-Verbindung“ (Local Area Connection) sehen. Doppelklicken Sie auf diesen Eintrag.
4. Wählen Sie **Eigenschaften**.
5. Überprüfen Sie, ob der „Client für Microsoft-Netzwerke“ und das „Internetprotokoll (TCP/IP)“ vorhanden sind. Wenn nicht, wählen Sie **Installieren** und fügen Sie sie hinzu.
6. Wählen Sie „Internetprotokoll (TCP/IP)“, klicken Sie auf **Eigenschaften** und stellen Sie sicher, dass „IP-Adresse automatisch beziehen“ ausgewählt ist.
7. Klicken Sie auf **OK** und schließen Sie alle Fenster zu den Netzwerk- und DFÜ-Verbindungen.
8. Starten Sie Ihren PC jetzt neu.

DHCP-Konfiguration von TCP/IP unter Windows XP, 2000 oder NT4

Sie werden feststellen, dass sich die Verfahren bei der Verwendung von DHCP zur Konfiguration von TCP/IP in den verschiedenen Windows-Systemen ähnlich sind.

Die folgenden Schritte führen Sie durch den Konfigurationsvorgang für jede dieser Windows-Versionen.

DHCP-Konfiguration von TCP/IP unter Windows XP

1

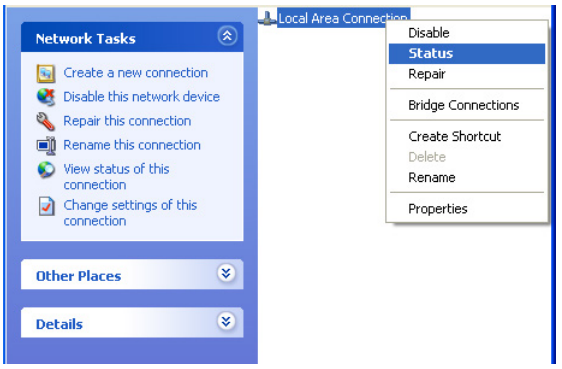
Suchen Sie das Symbol **Netzwerkumgebung**.

- Wählen Sie im Startmenü von Windows XP die **Systemsteuerung**.
- Wählen Sie in der Systemsteuerung das Symbol **Netzwerkverbindungen**. Damit gelangen Sie zum nächsten Schritt.

2

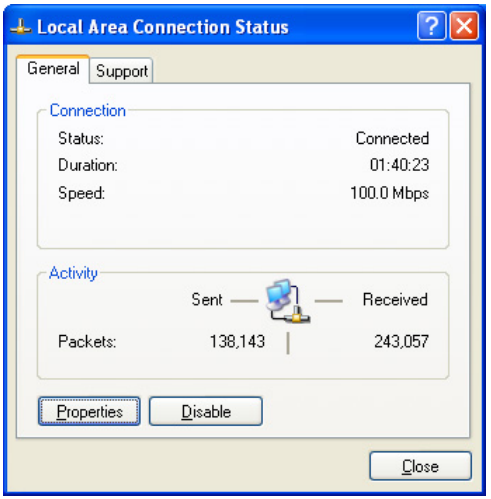
- Sie sehen jetzt das Fenster „Netzwerkverbindungen“.

  Rechts neben dem Fenster befindet sich die Liste aller auf dem PC eingerichteten Netzwerkverbindungen.
- Rechtsklicken Sie auf die Verbindung, die Sie verwenden möchten, und wählen Sie **Status**.



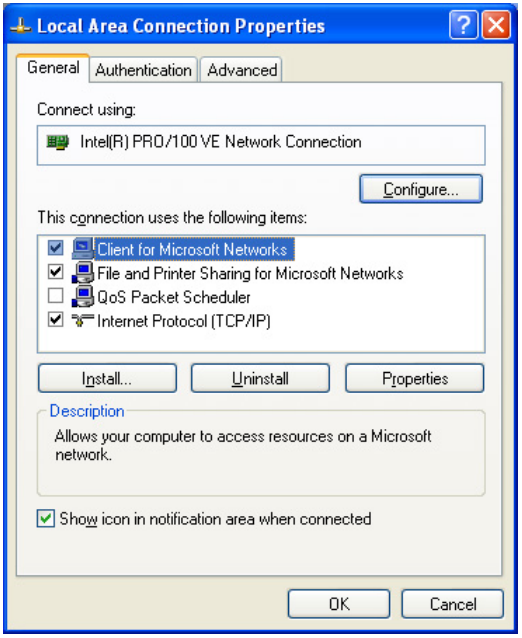
3

- Damit müssten Sie das Fenster mit dem Verbindungsstatus des LAN (Local Area Network) aufrufen. In diesem Fenster werden die Werte für Verbindungsstatus (Status), Dauer (Duration), Übertragungsrate (Speed) und Aktivität (Activity) angezeigt.
- Sie müssen Zugriffsrechte als Administrator haben, um dieses Fenster verwenden zu können.
- Klicken Sie auf die Schaltfläche **Eigenschaften** (Properties), um sich Einzelheiten zur Verbindung anzeigen zu lassen.



4

- Die TCP/IP-Details werden auf der Registerkarte „Netzwerkunterstützung“ (Support) angezeigt.
- Wählen Sie **Internetprotokoll** (Internet Protocol) und klicken Sie auf **Eigenschaften** (Properties), um sich die Informationen zur Konfiguration anzusehen**.**

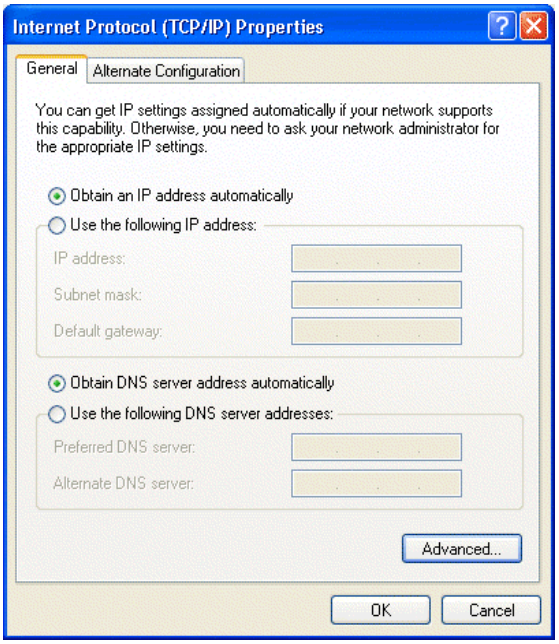


5

- Achten Sie darauf, dass die Optionsschaltfläche **IP-Adresse automatisch beziehen** (Obtain an IP address automatically) ausgewählt ist.
- Achten Sie darauf, dass die Optionsschaltfläche **DNS-Serveradresse automatisch beziehen** (Obtain DNS address automatically) ausgewählt ist.
- Klicken Sie auf die Schaltfläche **OK**.

Damit ist die DHCP-Konfiguration von TCP/IP unter Windows XP abgeschlossen.

Wiederholen Sie diese Schritte auf jedem PC im Netzwerk, der diese Windows-Version verwendet.


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

DHCP-Konfiguration von TCP/IP unter Windows 2000

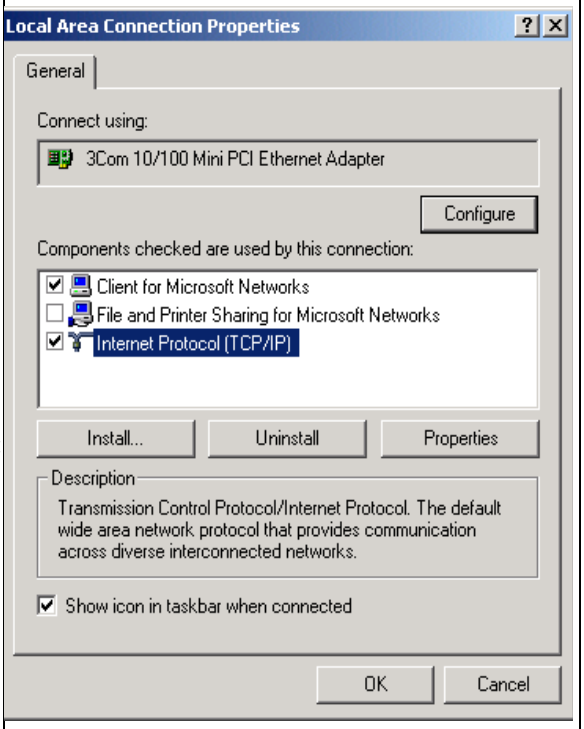
Auch hier wird nach der Installation der Netzwerkkarte TCP/IP für Windows 2000 konfiguriert. TCP/IP wird in der Regel standardmäßig hinzugefügt und auf DHCP eingestellt, ohne dass Sie die Konfiguration vornehmen müssen. Falls dabei jedoch Probleme auftreten, befolgen Sie die nachstehenden Schritte, um TCP/IP mit DHCP für Windows 2000 zu konfigurieren.

1

- Doppelklicken Sie auf das Symbol **Netzwerkumgebung** auf dem Windows-Desktop. Damit wird ein Fenster namens „Netzwerk- und DFÜ-Verbindungen“ aufgerufen.
- Rechtsklicken Sie auf **LAN-Verbindung** und wählen Sie **Eigenschaften**.

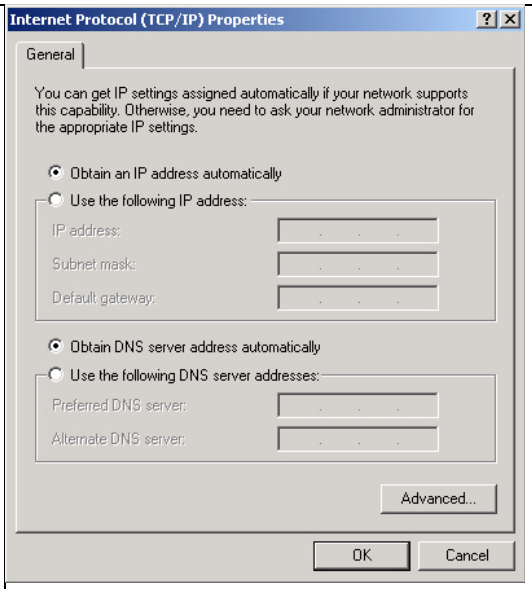
2

- Daraufhin erscheint das Dialogfeld mit den Eigenschaften der LAN-Verbindung (Local Area Connection Properties).
- Achten Sie darauf, dass im Feld **Verbindung herstellen unter Verwendung von:** (Connect using:) die richtige Netzwerkkarte ausgewählt ist.
- Im Feld **Aktivierte Komponenten werden von dieser Verbindung verwendet:** (Components checked are used by this connection:) sollten mindestens die folgenden beiden Objekte angezeigt und ausgewählt sein:
  - Client für Microsoft-Netzwerke (Client for Microsoft Networks) und
  - Internetprotokoll (TCP/IP) (Internet Protocol (TCP/IP))
- Klicken Sie auf **OK**.



3

- Wählen Sie **Internetprotokoll (TCP/IP)** und klicken Sie auf **Eigenschaften** (Properties), um das Dialogfeld mit den Eigenschaften des Internetprotokolls (TCP/IP) (Internet Protocol (TCP/IP) Properties) zu öffnen.
- Überprüfen Sie Folgendes:
  - **IP-Adresse automatisch beziehen** (Obtain an IP address automatically) ist ausgewählt.
  - **DNS-Serveradresse automatisch beziehen** (Obtain DNS server address automatically) ist ausgewählt.
- Klicken Sie auf **OK**, um zu den Eigenschaften der LAN-Verbindung zurückzukehren.

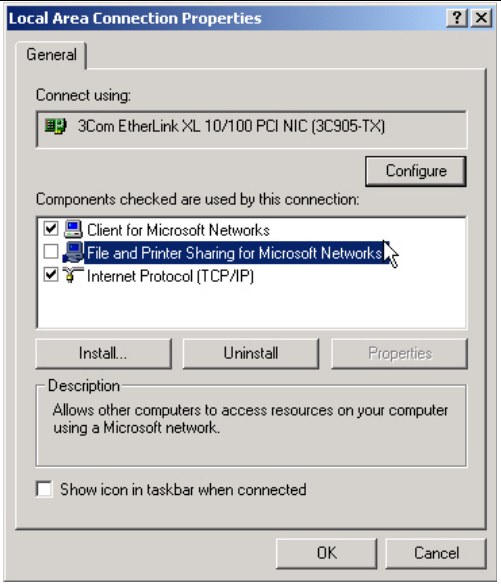

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

4

- Klicken Sie erneut auf **OK**, um den Konfigurationsvorgang für Windows 2000 abzuschließen.

Starten Sie den PC neu.

Wiederholen Sie diese Schritte auf jedem PC im Netzwerk, der diese Windows-Version verwendet.



DHCP-Konfiguration von TCP/IP unter Windows NT4

Nach der Installation der Netzwerkkarte müssen Sie die TCP/IP-Umgebung für Windows NT 4.0 konfigurieren. Befolgen Sie die nachstehende Anleitung, um TCP/IP mit DHCP unter Windows NT 4.0 zu konfigurieren.

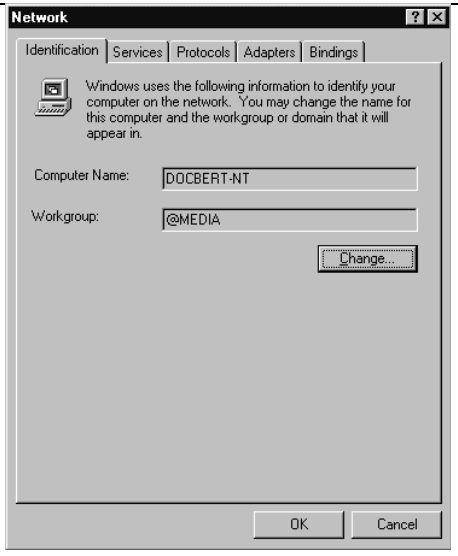
1

- Wählen Sie im Startmenü **Einstellungen** und dann **Systemsteuerung**. Damit wird das Systemsteuerungsfenster angezeigt.

2

- Doppelklicken Sie im Systemsteuerungsfenster auf das Symbol **Netzwerk**.

  Daraufhin wird das Netzwerkfenster (Network) angezeigt.
- Wählen Sie zum Fortfahren die Registerkarte „Protokolle“ (Protocols).



3

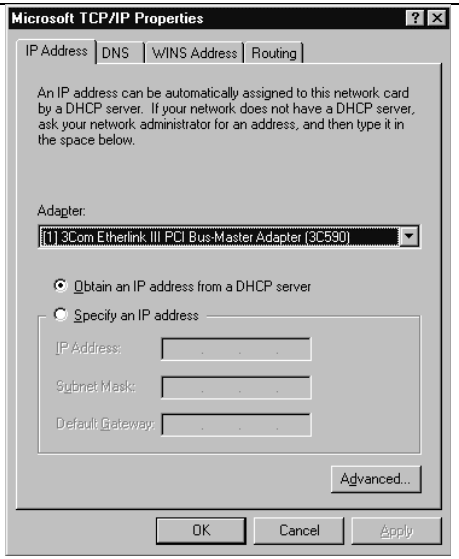
- Markieren Sie das **TCP/IP-Protokoll** (TCP/IP Protocol) im Feld „Netzwerkprotokolle“ (Network Protocols) und klicken Sie auf die Schaltfläche **Eigenschaften** (Properties).

4

- Daraufhin wird das Dialogfeld mit den Eigenschaften von TCP/IP (TCP/IP Properties) angezeigt.
- Klicken Sie auf die Registerkarte "IP-Adresse" (IP Address).
- Wählen Sie die Optionsschaltfläche **IP-Adresse von einem DHCP-Server beziehen** (Obtain an IP address from a DHCP server).
- Klicken Sie auf **OK**. Damit ist die Konfiguration von TCP/IP unter Windows NT abgeschlossen.

Starten Sie den PC neu.

Wiederholen Sie diese Schritte auf jedem PC im Netzwerk, der diese Windows-Version verwendet.


Microsoft TCP/IP Properties
IP Address
DNS
WINS Address
Routing
An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Adapter:
[1] 3Com Etherlink III PCI Bus-Master Adapter (3C590)
Obtain an IP address from a DHCP server
Specify an IP address
IP Address:
Subnet Mask:
Default Gateway:
Advanced...
OK
Cancel
Apply

Überprüfen der TCP/IP-Eigenschaften unter Windows XP, 2000 und NT4

So überprüfen Sie die TCP/IP-Konfiguration Ihres PCs:

1. Klicken Sie in der Windows-Taskleiste auf die Schaltfläche **Start** und klicken Sie dann auf **Ausführen**.

   Damit wird das Fenster „Ausführen“ geöffnet.

2. Geben Sie **`cmd`** ein und klicken Sie dann auf **OK**.

   Damit öffnen Sie ein Befehlsfenster.

3. Geben Sie **`ipconfig /all`** ein.

   Daraufhin wird Ihre IP-Konfiguration angezeigt; sie sollte mit den unten aufgeführten Werten übereinstimmen, wenn Sie die Standard-TCP/IP-Einstellungen verwenden, die NETGEAR für eine Verbindung über einen Router oder ein Gateway empfiehlt:

   - Die IP-Adresse liegt zwischen 192.168.1.2 und 192.168.1.254.
   - Die Subnetzmaske lautet 255.255.255.0.

- Die Standardgateway-Adresse lautet 192.168.1.1.

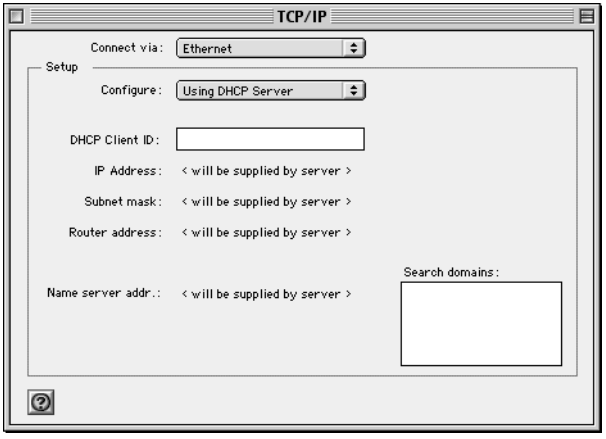
4. Geben Sie **`exit`** ein.

Einrichten eines Apple-Computers für den TCP/IP-Netzwerkbetrieb

Seit System 7 ist TCP/IP bereits auf dem Apple installiert. Auf jedem Apple-Computer im Netzwerk müssen Sie TCP/IP für die Verwendung von DHCP einrichten.

Mac OS 8.6 oder 9.x

1. Wählen Sie im Apfelmenü **Kontrollfelder** und dann **TCP/IP**.
   Daraufhin wird das TCP/IP-Kontrollfeld geöffnet:



2. Wählen Sie im Feld „Verbindung“ (Connect via) die Netzwerk-Schnittstelle Ihres Apple.
3. Wählen Sie im Feld „Konfigurationsmethode“ (Configure) **DHCP Server**.
   Das Feld „DHCP Client ID“ können Sie leer lassen.
4. Schließen Sie das TCP/IP-Kontrollfeld.
5. Wiederholen Sie diesen Vorgang auf jedem Apple-Computer in Ihrem Netzwerk.

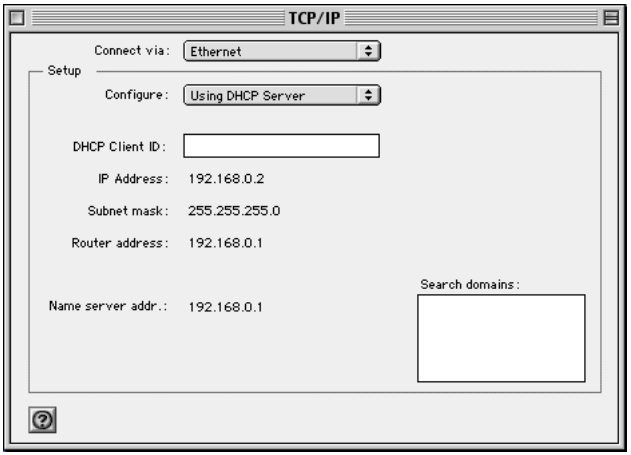
Mac OS X

1. Wählen Sie im Apfelmenü **Systemeinstellungen** und dann **Netzwerk**.

2. Falls sie noch nicht ausgewählt ist, wählen Sie in der Liste „Zeigen“ die Option **Ethernet (integriert)**.
3. Falls sie noch nicht ausgewählt ist, wählen Sie auf der Registerkarte „TCP/IP“ die Option **DHCP**.
4. Klicken Sie auf **Sichern**.

Überprüfen der TCP/IP-Eigenschaften bei Apple-Computern

Nachdem Sie Ihren Rechner konfiguriert und neu gestartet haben, können Sie die TCP/IP-Konfiguration überprüfen, indem Sie wieder zum TCP/IP-Kontrollfeld gehen. Wählen Sie im Apfelmenü **Kontrollfelder** und dann **TCP/IP**.



Das Fenster wird aktualisiert, um Ihre Einstellungen anzuzeigen; sie sollten mit den unten aufgeführten Werten übereinstimmen, wenn Sie die Standard-TCP/IP-Einstellungen verwenden, die NETGEAR empfiehlt:

- Die IP-Adresse liegt zwischen 192.168.1.2 und 192.168.1.254.
- Die Teilnetzmaske lautet 255.255.255.0.
- Die Router Adresse lautet 192.168.1.1.

Wenn Sie diese Werte nicht sehen, müssen Sie Ihren Apple möglicherweise neu starten oder eine andere Option für die Konfigurationsmethode wählen, bevor Sie wieder auf **DHCP Server** umschalten.

Überprüfen der Bereitschaft des Internetzugangs

Um Breitbandzugriff auf das Internet zu erhalten, müssen Sie bei einem Internetdienstanbieter einen Vertrag über Internetzugang für Einzelbenutzer per Kabel- oder DSL-Modem abschließen. Das Modem muss ein eigenständiges Gerät sein (keine Karte) und über einen Ethernet-Anschluss verfügen, der mit einer Netzwerkkarte im Computer verbunden werden kann. Ihre Firewall unterstützt keine Breitbandmodems mit USB-Verbindung.

Bei einem Internetzugang für Einzelbenutzer liefert Ihr Internetdienstanbieter Informationen zur TCP/IP-Konfiguration für einen Computer. Normalerweise wird ein Großteil der Konfigurationsdaten beim ersten Systemstart des PCs mit Verbindung zum ISP dynamisch zugewiesen und Sie brauchen diese dynamischen Informationen nicht zu kennen.

Wenn die Internetverbindung jedoch von mehreren Computern gemeinsam verwendet werden soll, übernimmt Ihre Firewall die Rolle des einzelnen PCs und Sie müssen sie mit den TCP/IP-Informationen einrichten, die sonst der PC nutzen würde. Wenn der Internetport der Firewall mit dem Breitbandmodem verbunden ist, wird die Firewall vom ISP als einzelner PC aufgefasst. Die Firewall sorgt dann dafür, dass sich die PCs im lokalen Netzwerk als einzelner PC ausgeben, um über das Breitbandmodem auf das Internet zuzugreifen. Die Firewall wendet dazu eine Methode namens Netzwerk-Adressumsetzung (kurz NAT) oder IP-Maskierung an.

Werden Anmeldeprotokolle verwendet?

Bei manchen Internetdienstanbietern ist ein besonderes Anmeldeprotokoll erforderlich, bei dem Sie einen Benutzernamen und ein Passwort eingeben müssen, um auf das Internet zugreifen zu können. Wenn Sie normalerweise ein Programm wie WinPOET oder EnterNet für die Anmeldung im Internet verwenden, nutzt Ihr PC PPP over Ethernet (PPPoE) für den Internetzugang.

Bei der Konfiguration des Routers müssen Sie Ihren Anmeldenamen und das Passwort in die Konfigurationsmenüs des Routers eingeben. Nach der Konfiguration des Netzwerks und der Firewall führt die Firewall bei Bedarf die Anmeldung durch und Sie brauchen das Anmeldeprogramm nicht mehr auf dem PC auszuführen. Das Anmeldeprogramm braucht jedoch nicht deinstalliert zu werden.

Wie lauten Ihre Konfigurationsdaten?

Immer mehr Internetdienstanbieter weisen Konfigurationsdaten dynamisch zu. Wenn Ihr ISP die Konfigurationsdaten jedoch nicht dynamisch zuweist, sondern eine feste Konfiguration verwendet, sollten Sie die folgenden Grunddaten zur Konfiguration von Ihrem ISP erhalten haben:

- Eine IP-Adresse und Subnetzmaske
- Eine Gateway-IP-Adresse, die der Adresse des Routers Ihres ISP entspricht
- Mindestens eine IP-Adresse für DNS-Server
- Host- und Domainnamen

  Der vollständige Servername für Ihren Internetzugang kann beispielsweise folgendermaßen aussehen:

  `mail.xxx.yyy.de`

  In diesem Beispiel lautet der Domainname `xxx.yyy.de`.

Wenn diese Daten von Ihrem ISP ganz oder teilweise dynamisch bereitgestellt werden, ruft Ihre Firewall sie automatisch ab.

Wenn ein Techniker Ihres Internetdienstanbieters Ihren PC bei der Installation des Breitbandmodems konfiguriert hat oder wenn Sie ihn nach Anleitung Ihres Dienstanbieters konfiguriert haben, sollten Sie die aktuellen Konfigurationsdaten aus dem Fenster mit den TCP/IP-Eigenschaften für das Netzwerk Ihres PCs bzw. dem TCP/IP-Kontrollfeld Ihres Apple-Computers für die Konfiguration Ihrer Firewall verwenden. Diese Verfahren werden im Folgenden beschrieben.

Ermitteln der ISP-Konfigurationsdaten für Windows-Computer

Wie oben erwähnt, müssen Sie möglicherweise die Konfigurationsdaten von Ihrem PC ermitteln, um sie bei der Konfiguration des WPN824 Routers einsetzen zu können. Dieses Verfahren ist nur dann erforderlich, wenn Ihr Internetdienstanbieter die Daten für den Internetzugang nicht dynamisch zuweist.

Zum Bezug dieser Daten müssen Sie die Firewall für den Internetzugang konfigurieren:

1. Klicken Sie in der Windows-Taskleiste auf die Schaltfläche **Start**, wählen Sie **Einstellungen** und klicken Sie dann auf **Systemsteuerung**.
2. Doppelklicken Sie auf das Symbol **Netzwerk**.

   Daraufhin wird das Fenster „Netzwerk“ mit einer Liste der installierten Komponenten geöffnet.
3. Wählen Sie **TCP/IP** und klicken Sie dann auf **Eigenschaften**.

   Daraufhin wird das Dialogfeld mit den Eigenschaften von TCP/IP angezeigt.
4. Wählen Sie die Registerkarte „IP-Adresse“.

   Wenn eine IP-Adresse und Subnetzmaske angezeigt werden, notieren Sie diese Daten. Wenn eine Adresse vorhanden ist, verwendet Ihr PC eine feste (statische) IP-Adresse für den Internetzugang. Ist keine Adresse vorhanden, nutzt Ihr PC eine dynamisch zugewiesene IP-Adresse. Klicken Sie auf **IP-Adresse automatisch beziehen**.
5. Wählen Sie die Registerkarte „Gateway“.

Wenn unter den installierten Gateways eine IP-Adresse angegeben ist, notieren Sie diese Adresse. Es handelt sich dabei um die Gateway-Adresse Ihres ISPs. Wählen Sie diese Adresse und klicken Sie dann auf **Entfernen**, um sie zu löschen.

6. Wählen Sie die Registerkarte „DNS-Konfiguration“.

   Wenn DNS-Serveradressen angezeigt werden, notieren Sie diese Adressen. Falls sich Angaben im Feld mit den Host- oder Domainnamen befinden, notieren Sie diese. Klicken Sie auf **DNS deaktivieren**.

7. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern, und schließen Sie das Dialogfeld mit den TCP/IP-Eigenschaften.

   Damit kehren Sie zum Fenster „Netzwerk“ zurück.

8. Klicken Sie auf **OK**.

9. Starten Sie Ihren PC nach der entsprechenden Aufforderung neu. Sie können auch aufgefordert werden, Ihre Windows-CD einzulegen.

Ermitteln der ISP-Konfigurationsdaten für Apple-Computer

Wie oben erwähnt, müssen Sie möglicherweise die Konfigurationsdaten von Ihrem Apple ermitteln, um sie bei der Konfiguration des WPN824 Routers einsetzen zu können. Dieses Verfahren ist nur dann erforderlich, wenn Ihr Internetdienstanbieter die Daten für den Internetzugang nicht dynamisch zuweist.

Zum Bezug dieser Daten müssen Sie die Firewall für den Internetzugang konfigurieren:

1. Wählen Sie im Apfelmenü **Kontrollfelder** und dann **TCP/IP**.

   Daraufhin wird das TCP/IP-Kontrollfeld mit einer Liste der Konfigurationseinstellungen geöffnet: Wenn als Konfigurationsmethode **DHCP-Server** angegeben ist, verwendet Ihr Apple eine dynamisch zugewiesene IP-Adresse. Schließen Sie in diesem Fall das Kontrollfeld und überspringen Sie den Rest dieses Abschnitts.

2. Wenn eine IP-Adresse und Teilnetzmaske angezeigt werden, notieren Sie diese Informationen.

3. Wenn unter der Router-Adresse eine IP-Adresse angegeben ist, notieren Sie diese Adresse. Es handelt sich dabei um die Gateway-Adresse Ihres ISPs.

4. Falls Nameserver-Adressen angezeigt werden, notieren Sie diese Adressen. Es handelt sich dabei um die DNS-Adressen Ihres ISPs.

5. Falls das Feld „Suchpfad: Lokale Domain“ Informationen enthält, notieren Sie diese.

6. Ändern Sie die Einstellung unter „Konfigurationsmethode“ zu **DHCP Server**.

7. Schließen Sie das TCP/IP-Kontrollfeld.

Neustarten des Netzwerks

Sobald Sie Ihre Computer für den Zugang über die Firewall eingerichtet haben, müssen Sie das Netzwerk zurücksetzen, damit die Geräte miteinander kommunizieren können. Starten Sie alle mit der Firewall verbundenen Computer neu.

Wenn Sie alle Computer für den TCP/IP-Netzwerkbetrieb eingerichtet, sie neu gestartet und mit dem lokalen Netzwerk Ihres WPN824 Routers verbunden haben, sind Sie bereit für den Zugriff auf und die Konfiguration der Firewall.

Anhang D
Grundlagen drahtloser Netzwerke

Dieses Kapitel gibt einen Überblick über drahtlose Netzwerke.

Überblick über drahtlose Netzwerke

Der WPN824 Router erfüllt die Standards 802.11b und 802.11g für drahtlose Netzwerke (kurz WLANs) des IEEE (Institute of Electrical and Electronics Engineers). Bei einer drahtlosen Verbindung des Typs 802.11b oder g werden die Daten über das DSSS-Verfahren (Direct Sequence Spread Spectrum) verschlüsselt und im lizenzfreien Frequenzband bei 2,4 GHz übertragen. Die maximale Übertragungsrate für drahtlose Verbindungen des Typs 802.11b beträgt 11 MBit/s. Wenn das Funksignal schwach ist oder Interferenzen entdeckt werden, wird die Übertragungsrate jedoch automatisch von 11 MBit/s zunächst auf 5,5, dann auf 2 und schließlich auf 1 MBit/s gesenkt. Beim Standard 802.11g liegen die automatisch erfassten Übertragungsraten bei 1; 2; 5,5; 6; 9; 12; 18; 24; 36; 48; 54 und im Turbomodus bei 108 MBit/s.

Die WECA (Wireless Ethernet Compatibility Alliance, vgl. *http://www.wi-fi.net*), eine Gruppe, die Branchenstandards für die Kompatibilität von 802.11-Geräten festlegt, bezeichnet den Standard 802.11 auch als „Wireless Ethernet“ oder „Wi-Fi“. Der Standard 802.11 bietet zwei Modi zum Betrieb eines drahtlosen Netzwerks, den Ad-hoc-Modus und den Infrastruktur-Modus.

Infrastruktur-Modus

Mit einem Wireless Access Point können Sie das WLAN im Infrastruktur-Modus betreiben. Dieser Modus bietet drahtlose Verbindungen für eine Vielzahl von drahtlosen Geräten, die sich innerhalb einer festgelegten Reichweite befinden und über eine Antenne mit den Hosts des drahtlosen Netzwerks kommunizieren.

Im Infrastruktur-Modus wandelt der Wireless Access Point Funkdaten in Daten für das kabelgebundene Netzwerk um. Er bildet also eine Bridge zwischen dem verdrahteten LAN und drahtlosen Clients. Der Funkbereich des drahtlosen Netzwerks kann vergrößert werden, indem mehrere Access Points über einen verkabelten Netzwerk-Backbone verbunden werden. Wenn ein mobiles Gerät die Funkzelle eines Access Points verlässt, bewegt es sich in die Funkzelle eines anderen. So können drahtlose Clients sich frei von einem Access-Point-Bereich zum nächsten bewegen, ohne dass dabei die Verbindung unterbrochen wird.

Ad-hoc-Modus (Peer-to-Peer-Arbeitsgruppe)

In einem Ad-hoc-Netzwerk werden Computer je nach Bedarf verbunden. Es gibt also keinerlei Struktur oder feste Stationen in diesem Netzwerk – in der Regel kann jeder Host mit allen anderen Hosts kommunizieren. Bei dieser Konfiguration gibt es keinen Access Point. In diesem Modus können Sie schnell eine kleine drahtlos verbundene Arbeitsgruppe einrichten, deren Mitglieder dann über das Microsoft-Netzwerk ihrer jeweiligen Windows-Betriebssysteme Daten austauschen und Drucker gemeinsam nutzen können. Manche Hersteller bezeichnen Ad-hoc-Netzwerke auch als „Peer-to-Peer-Netzwerke“.

In dieser Betriebsart werden Datenpakete direkt von den Sende- an die Empfangsstationen gesendet. Solange sich die Stationen in Funkreichweite zueinander befinden, ist dies die einfachste und preisgünstigste Methode zur Einrichtung eines drahtlosen Netzwerks.

Netzwerkname: ESSID (Extended Service Set Identifier)

Die ESSID ist eine von zwei Arten von SSID (Service Set Identifier). In einem drahtlosen Ad-hoc-Netzwerk ohne Access Points wird eine BSSID (Basic Service Set Identifier) verwendet. In einem drahtlosen Infrastruktur-Netzwerk, das einen Access Point enthält, wird die ESSID verwendet, die manchmal auch einfach als SSID bezeichnet wird.

Eine SSID ist ein aus maximal 32 alphanumerischen Zeichen bestehender Code, der den Namen des WLANs festlegt. Manche Hersteller bezeichnen die SSID auch als „Netzwerknamen“. Damit die drahtlosen Geräte in einem Netzwerk miteinander kommunizieren können, müssen alle Geräte mit derselben SSID konfiguriert werden.

Die ESSID wird normalerweise von einem Access Point gesendet. Die drahtlose Station kann manchmal mit einer ESSID namens **ANY** konfiguriert werden. Bei dieser Konfiguration versucht die drahtlose Station, sich dem Access Point mit dem stärksten Funksignal zuzuordnen. Voraussetzung dafür ist, dass sowohl der Access Point als auch die drahtlose Station zur Authentifizierung Open System verwenden.

Authentifizierung und WEP-Datenverschlüsselung

Da keine physische Verbindung zwischen den Hosts besteht, sind drahtlose Verbindungen anfällig für Eindringlinge und Datendiebstahl. Um ein gewisses Maß an Sicherheit zu bieten, wurden im Standard IEEE 802.11 die folgenden beiden Authentifizierungsmethoden definiert:

- **Open System**. Bei der Authentifizierung über Open System kann ein drahtloser Computer sich jedem Netzwerk anschließen und alle unverschlüsselten Nachrichten empfangen.

- **Shared Key**. Bei der Authentifizierung über Shared Key können sich nur PCs, die über den richtigen Authentifizierungsschlüssel verfügen, dem Netzwerk anschließen. Drahtlose IEEE 802.11-Geräte sind standardmäßig so konfiguriert, dass sie mit Open System arbeiten.

Wenn die Geräte für den Authentifizierungsmodus Shared Key konfiguriert werden, wird zur Datenverschlüsselung WEP (Wired Equivalent Privacy) verwendet.

802.11-Authentifizierung

Im Standard 802.11 wurden mehrere Dienste definiert, die die Kommunikation von zwei 802.11-Geräten bestimmen. Eine 802.11-Station kann erst über einen Access Point, wie er im WPN824 integriert ist, mit einem Netzwerk kommunizieren, wenn die folgenden Schritte geschehen sind:

1. Die drahtlose Station wird eingeschaltet.
2. Die Station sucht nach Nachrichten von Access Points in ihrer Reichweite.
3. Die Station empfängt eine Nachricht von einem Access Point mit einer passenden SSID.
4. Die Station sendet eine Authentifizierungsanforderung an den Access Point.
5. Der Access Point authentifiziert die Station.
6. Die Station sendet eine Zuordnungsanforderung an den Access Point.
7. Der Access Point ordnet sich der Station zu.
8. Die Station kann nun über den Access Point mit dem Netzwerk kommunizieren.

Erst wenn die Station durch den Access Point authentifiziert wurde, kann sie sich dem Access Point zuordnen und mit dem Netzwerk kommunizieren. Im Standard IEEE 802.11 wurden zwei Arten der Authentifizierung festgelegt: Open System und Shared Key.

- Bei der Authentifizierung über Open System kann sich jedes Gerät dem Netzwerk anschließen, dessen SSID mit der SSID des Access Points übereinstimmt. Wenn als SSID „ANY“ ausgewählt ist, kann das entsprechende Gerät sich unabhängig von der SSID jedem verfügbaren Access Point in Reichweite zuordnen.
- Bei der Shared-Key-Authentifizierung müssen die Station und der Access Point denselben WEP-Schlüssel haben, damit eine Authentifizierung möglich ist. Die beiden Authentifizierungsmethoden werden im Folgenden näher erklärt.

Open-System-Authentifizierung

Wenn zwei Geräte sich über Open System authentifizieren, läuft der Verbindungsaufbau zum Netzwerk wie folgt ab:

1. Die Station sendet eine Authentifizierungsanforderung an den Access Point.

2. Der Access Point authentifiziert die Station.
3. Die Station ordnet sich dem Access Point zu und schließt sich dem Netzwerk an.

Dieser Vorgang ist in der Abbildung unten dargestellt.

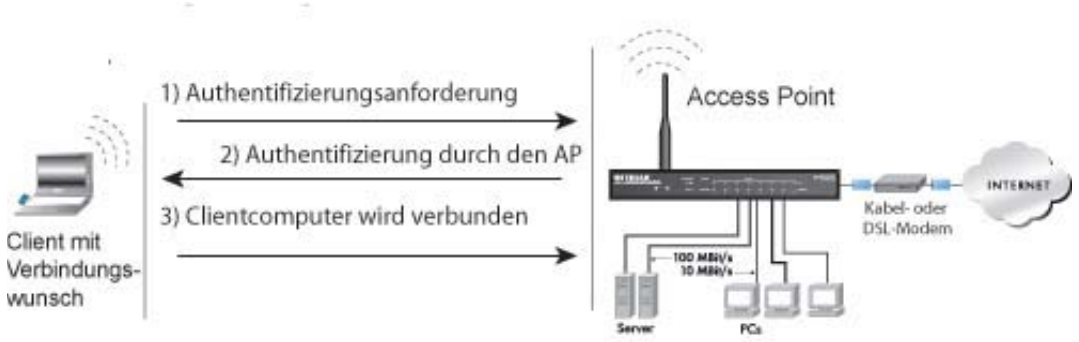


Abbildung D-1: Open-System-Authentifizierung

Shared-Key-Authentifizierung

Wenn zwei Geräte sich per Shared Key authentifizieren, läuft der Verbindungsaufbau zum Netzwerk wie folgt ab:

1. Die Station sendet eine Authentifizierungsanforderung an den Access Point.
2. Der Access Point sendet eine Testnachricht an die Station.
3. Die Station verwendet zum Verschlüsseln der Testnachricht den konfigurierten 64-Bit- oder 128-Bit-Standardschlüssel und sendet den verschlüsselten Text dann an den Access Point.
4. Der Access Point entschlüsselt den verschlüsselten Text mit Hilfe des konfigurierten WEP-Schlüssels, der dem Standardschlüssel der Station entspricht. Der Access Point vergleicht den entschlüsselten Text mit dem ursprünglichen Text. Wenn der entschlüsselte Text mit dem ursprünglichen Text übereinstimmt, verwenden der Access Point und die Station denselben WEP-Schlüssel und der Access Point authentifiziert die Station.
5. Die Station stellt eine Verbindung zum Netzwerk her.

Wenn der entschlüsselte Text nicht mit dem ursprünglichen Text übereinstimmt (und der Access Point und die Station demnach nicht denselben WEP-Schlüssel verwenden), verweigert der Access Point der Station die Authentifizierung und die Station kann weder mit dem 802.11-Netzwerk noch mit dem kabelgebundenen Netzwerk kommunizieren.

Dieser Vorgang ist in der Abbildung unten dargestellt.

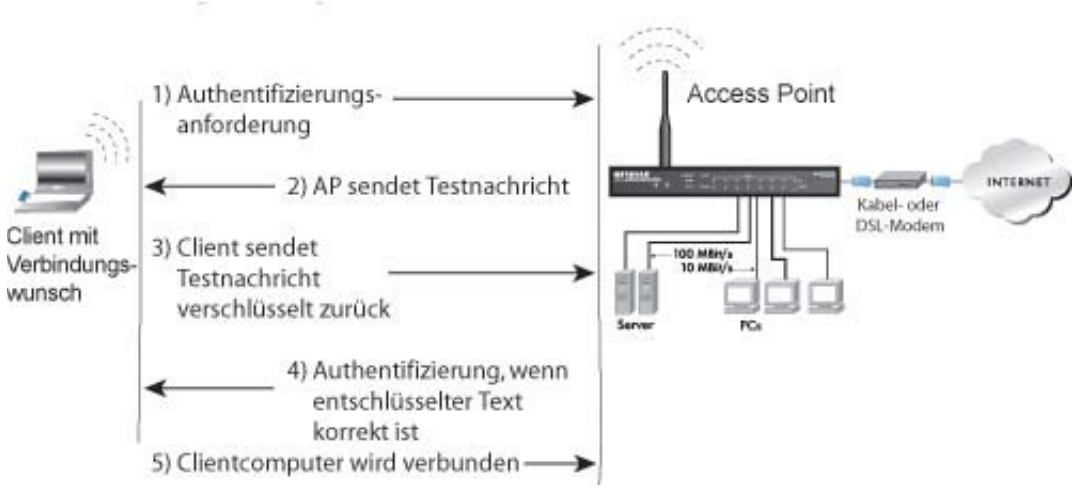


Abbildung D-2: Shared-Key-Authentifizierung

Überblick über die WEP-Parameter

Bevor Sie bei einem 802.11-Netzwerk WEP aktivieren, sollten Sie überlegen, welche Art der Verschlüsselung Sie benötigen und wie groß der Schlüssel sein soll. Bei 802.11-Geräten gibt es in der Regel drei Optionen für die WEP-Verschlüsselung:

1. **WEP wird überhaupt nicht verwendet:** Das 802.11-Netzwerk verschlüsselt keinerlei Daten. Zur Authentifizierung wird Open System verwendet.

2. **WEP wird zur Verschlüsselung verwendet:** Sendende 802.11-Geräte verschlüsseln den Datenbestandteil jedes Datenpakets, das versendet wird, mit einem konfigurierten WEP-Schlüssel. Das Empfangsgerät entschlüsselt die Daten mit demselben WEP-Schlüssel. Zur Authentifizierung wird Open System verwendet.

3. **WEP wird zur Authentifizierung und Verschlüsselung verwendet:** Sendende 802.11-Geräte verschlüsseln den Datenbestandteil jedes Datenpakets, das versendet wird, mit einem konfigurierten WEP-Schlüssel. Das Empfangsgerät entschlüsselt die Daten mit demselben WEP-Schlüssel. Zur Authentifizierung im drahtlosen Netzwerk wird die Shared-Key-Authentifizierung verwendet.

Hinweis: Bei manchen 802.11-Access-Points ist es zudem möglich, **WEP nur zur Authentifizierung zu verwenden** (Shared-Key-Authentifizierung ohne Datenverschlüsselung).

Schlüsseltiefe

Der Standard IEEE 802.11 unterstützt zwei Arten der WEP-Verschlüsselung: 64 Bit und 128 Bit.

Bei der 64-Bit-WEP-Datenverschlüsselung können 5 Zeichen (40 Bits) eingegeben werden. Dazu kommen 24 voreingestellte Bits, die zusammen mit den 40 Bits einen 64-Bit-Schlüssel ergeben. (Die voreingestellten 24 Bits können nicht vom Benutzer geändert werden.) Dieser Schlüssel wird zur Verschlüsselung und Entschlüsselung aller Daten verwendet, die über das drahtlose Gerät versendet werden. Manche Hersteller bezeichnen die 64-Bit-WEP-Verschlüsselung als „40-Bit-WEP-Verschlüsselung“, da der Benutzer nur 40 Bits selbst bestimmen kann.

Bei der 128-Bit-WEP-Verschlüsselung können 104 Bits vom Benutzer bestimmt werden. Ähnlich wie bei der 64-Bit-WEP-Verschlüsselung sind die restlichen 24 Bits voreingestellt und können nicht vom Benutzer geändert werden. Manche Hersteller erlauben die Verwendung von Kennwörtern anstelle der komplizierten Hexadezimalcodes, um die Eingabe des Schlüssels zu erleichtern.

Die 128-Bit-Verschlüsselung ist sicherer als die 64-Bit-Verschlüsselung. Es kann jedoch sein, dass sie auf Grund von Exportvorschriften nicht überall verfügbar ist.

802.11-Geräte, die für 64-Bit-Verschlüsselung konfiguriert sind, unterstützen normalerweise bis zu vier WEP-Schlüssel. Jeder 64-Bit-WEP-Schlüssel besteht aus 5 Paaren von hexadezimalen Zeichen (0–9 and A–F). „12 34 56 78 90“ wäre ein Beispiel für einen 64-Bit-WEP-Schlüssel.

802.11-Geräte, die für 128-Bit-Verschlüsselung konfiguriert sind, unterstützen normalerweise vier WEP-Schlüssel. Produkte mancher Hersteller unterstützen allerdings nur einen 128-Bit-Schlüssel. Der 128-Bit-WEP-Schlüssel besteht aus 13 Paaren von hexadezimalen Zeichen (0–9 and A–F). „12 34 56 78 90 AB CD EF 12 34 56 78 90“ wäre ein Beispiel für einen 128-Bit-WEP-Schlüssel.

Tabelle D-1: Schlüsselgrößen

Schlüsselgröße	Anzahl hexadezimaler Zeichen	Beispiel für einen hexadezimalen Schlüssel
64-Bit (24+40)	10	4C72F08AE1
128-Bit (24+104)	26	4C72F08AE19D57A3FF6B260037

Hinweis: 802.11-Access-Points können normalerweise bis zu vier 128-Bit-WEP-Schlüssel speichern. Manche 802.11-Client-Adapter können jedoch nur einen derartigen Schlüssel speichern. Vergewissern Sie sich also, dass die Konfiguration Ihres 802.11-Access-Points mit der des Client-Adapters übereinstimmt.

WEP-Konfigurationsoptionen

Die WEP-Einstellungen müssen bei allen 802.11-Geräten, die zum selben drahtlosen Netzwerk gehören (also dieselbe SSID aufweisen), übereinstimmen. Wenn Ihre mobilen Clients also zwischen verschiedenen Access Points wechseln sollen, müssen die WEP-Einstellungen bei allen 802.11-Access-Points und allen 802.11-Client-Adaptern im Netzwerk identisch sein.

Hinweis: Achten Sie darauf, die Schlüssel beim Client-Adapter in derselben Reihenfolge einzugeben wie beim Access Point. WEP-Schlüssel 1 des Access Points muss also mit WEP-Schlüssel 1 des Client-Adapters übereinstimmen, WEP-Schlüssel 2 des Access Points mit WEP-Schlüssel 2 des Client-Adapters usw.

Hinweis: Access Point und Client-Adapter müssen nicht denselben Standardschlüssel verwenden. Die Hauptsache ist, dass die Schlüssel in derselben Reihenfolge erscheinen. Das heißt, wenn der Access Point WEP-Schlüssel 2 als Standardschlüssel für die Übertragung verwendet, kann ein Client-Adapter trotzdem WEP-Schlüssel 3 als Standardschlüssel für die Übertragung verwenden. Die zwei Geräte können dennoch miteinander kommunizieren, solange der WEP-Schlüssel 2 mit dem WEP-Schlüssel 2 des Client-Adapters identisch ist und der WEP-Schlüssel 3 des Access Points mit dem WEP-Schlüssel 3 des Client-Adapters.

Drahtlose Kanäle

Unten finden Sie eine Erläuterung der drahtlosen Frequenzen, die von 802.11b/g-Netzwerken verwendet werden.

Die Hosts in drahtlosen Netzwerken des Typs IEEE 802.11b/g kommunizieren über Funkfrequenzen im ISM-Band (Industrial, Scientific, and Medical) zwischen 2,4 und 2,5 GHz. Der Abstand zwischen den Kanälen beträgt jeweils 5 MHz. Auf Grund des Streuspektrums der Signale kommt es jedoch häufig vor, dass ein Host beim Versand von Signalen über einen bestimmten Kanal ein Frequenzspektrum von bis zu 12,5 MHz ober- und unterhalb der eigentlichen Kanalfrequenz nutzt. Dies führt zu Interferenzen, wenn in einer Umgebung zwei separate drahtlose Netzwerke nebeneinander bestehen, die aneinander grenzende Kanäle benutzen (z. B. Kanal 1 und 2). Die Verwendung von zwei Kanälen, die möglichst weit auseinander liegen, wird im Vergleich mit Netzwerken mit nahe beieinander liegenden Kanälen die Störungen deutlich verringern und die Leistung spürbar verbessern.

In Tabelle D-2 sind die Hochfrequenzkanäle aufgelistet, die von 802.11b/g-Netzwerken verwendet werden:

Tabelle D-2: 802.11b/g-Hochfrequenzkanäle

Kanal	Mittenfrequenz	Frequenzspanne
1	2412 MHz	2399,5 MHz–2424,5 MHz
2	2417 MHz	2404,5 MHz–2429,5 MHz
3	2422 MHz	2409,5 MHz–2434,5 MHz

Tabelle D-2: 802.11b/g-Hochfrequenzkanäle

Kanal	Mittenfrequenz	Frequenzspanne
4	2427 MHz	2414,5 MHz–2439,5 MHz
5	2432 MHz	2419,5 MHz–2444,5 MHz
6	2437 MHz	2424,5 MHz–2449,5 MHz
7	2442 MHz	2429,5 MHz–2454,5 MHz
8	2447 MHz	2434,5 MHz–2459,5 MHz
9	2452 MHz	2439,5 MHz–2464,5 MHz
10	2457 MHz	2444,5 MHz–2469,5 MHz
11	2462 MHz	2449,5 MHz–2474,5 MHz
12	2467 MHz	2454,5 MHz–2479,5 MHz
13	2472 MHz	2459,5 MHz–2484,5 MHz

Hinweis: In den einzelnen Ländern werden unterschiedliche Kanäle unterstützt. So werden in den USA und Kanada die Kanäle 1 bis 11 unterstützt, in Europa und Australien dagegen Kanäle 1 bis 13.

Als Abstand zwischen den Kanälen benachbarter drahtloser Netzwerke wird 25 MHz (5 Kanäle) empfohlen. So können Sie in Ihrem drahtlosen Netzwerk bis zu drei unterschiedliche Kanäle einsetzen. In den USA stehen nur 11 Kanäle zur Verfügung. Sie sollten also mit Kanal 1 beginnen und im Bedarfsfall auf Kanäle 6 und 11 erweitern, da diese Kanäle sich nicht überschneiden.

Sicherheit im drahtlosen Netzwerk mit WPA und WPA2

WPA (Wi-Fi Protected Access) und WPA2 sind Spezifikationen von standardbasierten, kompatiblen Sicherheitsfunktionen, die den Datenschutz und die Zugriffssteuerung bei bereits vorhandenen und bei künftigen WLAN-Systemen verbessern.

WEP wurde vom IEEE als optionale Sicherheitserweiterung für 802.11b-WLANs eingeführt, doch es zeigte sich bald, dass dieser Standard erhebliche Schwächen hatte. Angesichts dieser Situation stellte die Wi-Fi Alliance im Oktober 2002 eine neue Sicherheitsarchitektur vor, die die Mängel von WEP behebt. Dieser Standard war früher unter dem Namen „SSN“ (Safe Secure Network) bekannt und ist nicht nur mit bestehenden 802.11-Geräten kompatibel, sondern auch mit 802.11i, der neuen Sicherheitsarchitektur für drahtlose Netzwerke, die vom IEEE festgelegt wurde.

WPA und WPA2 bieten die folgenden Vorteile:

- Verbesserte Datensicherheit
- Stabile Schlüsselverwaltung
- Datenursprungsauthentifizierung
- Datenintegritätsschutz

Die Wi-Fi Alliance führt inzwischen bei WPA-Produkten Kompatibilitätszertifizierungstests durch. Seit August 2003 müssen alle neuen Wi-Fi-zertifizierten Produkte WPA unterstützen. NETGEAR implementiert WPA und WPA2 bei Client- und Access-Point-Produkten. Der Standard 802.11i wurde 2004 ratifiziert.

Worin unterscheidet sich WPA von WEP?

WEP ist ein Datenverschlüsselungsverfahren, das nicht zur Benutzerauthentifizierung gedacht ist. Die WPA-Benutzerauthentifizierung wird mit 802.1x und EAP (Extensible Authentication Protocol) implementiert. WPA erfordert die Unterstützung für 802.1x-Authentifizierung. Beim Standard 802.11 war die 802.1x-Authentifizierung optional. Nähere Informationen zum EAP finden Sie im IETF-Dokument RFC 2284.

Bei Verwendung von 802.11 WEP müssen alle Access Points und drahtlosen Client-Adapter eines drahtlosen Netzwerks denselben Verschlüsselungscode benutzen. Eines der größten Probleme des Standards 802.11 ist, dass das Ändern der Schlüssel sehr aufwendig ist. Wenn die WEP-Schlüssel nicht sehr häufig aktualisiert werden, können Unbefugte ein Netzwerk mit Hilfe eines Sniffing-Tools beobachten und innerhalb eines Tages die verschlüsselten Nachrichten entschlüsseln. Produkte, die ausschließlich auf dem Standard 802.11 basieren, bieten Administratoren keine effektive Methode zur Aktualisierung der Schlüssel.

Bei 802.11 ist die WEP-Verschlüsselung optional, bei WPA ist dagegen die Verschlüsselung über TKIP (Temporal Key Integrity Protocol) erforderlich. TKIP ersetzt WEP durch einen neuen Algorithmus, der stärker als der WEP-Algorithmus ist. Die für die Verschlüsselung erforderlichen Berechnungen können jedoch auch von älteren drahtlosen Geräten durchgeführt werden. TKIP bietet wichtige Verbesserungen zur Datenverschlüsselung, darunter eine Funktion zum paketweisen Ändern von Schlüsseln, die Nachrichtenintegritätsprüfung Michael (Message Integrity Check, MIC), einen erweiterten Initialisierungsvektor (IV) mit Sequenzierungsregeln und einen Mechanismus zur Neuverschlüsselung. Mit diesen Verbesserungen berücksichtigt TKIP alle bekannten Schwächen von WEP.

Worin unterscheidet sich WPA von WPA 2 (IEEE 802.11i)?

WPA ist aufwärts kompatibel mit den Sicherheitsanforderungen von WPA2. WPA ist eine Untergruppe von WPA2, die Elemente des ersten Entwurfs von 802.11i verwendet, darunter 802.1x und TKIP. Zu den Hauptelementen von WPA2, die nicht in WPA enthalten sind, gehören sicheres IBSS (Ad-hoc-Modus), Secure Fast Handoff (bei 802.11-VoIP-Telefonen) und verbesserte Verschlüsselungsprotokolle wie AES-CCMP. Diese Funktionen waren entweder noch in der Entwicklung oder für ihre Implementierung waren Hardware-Upgrades erforderlich.

Was sind die Hauptsicherheitsmerkmale von WPA und WPA2?

Die Standards WPA und WPA2 enthalten die folgenden Sicherheitsfunktionen:

- WPA- und WPA2-Authentifizierung
- WPA- und WPA2-Schlüsselverwaltung
  - TKIP (Temporal Key Integrity Protocol)
  - Michael/MIC (Message Integrity Code)
  - AES-Unterstützung (WPA2, Unterstützung durch die Hardware erforderlich)

Diese Funktionen werden unten näher beschrieben.

WPA/WPA2 berücksichtigt die meisten der bekannten Schwächen von WEP und ist in erster Linie für drahtlose Infrastrukturnetzwerke im Unternehmensbereich gedacht. Eine entsprechende Infrastruktur besteht aus Stationen, Access Points und Authentifizierungsservern (normalerweise RADIUS-Server). Auf dem RADIUS-Server sind Benutzeranmeldedaten wie Benutzernamen und Passwörter gespeichert oder er hat Zugriff auf diese. So kann der RADIUS-Server die Benutzer identifizieren, bevor sie auf das drahtlose Netzwerk zugreifen können.

Die Stärke von WPA/WPA2 liegt in einer integrierten Sequenz von Vorgängen, die 802.1x-/EAP-Authentifizierung sowie leistungsfähige Schlüsselverwaltungs- und Verschlüsselungstechniken umfassen. Zu den wichtigsten Vorgängen gehören:

- Feststellung der Netzwerksicherheitsfunktionen. Dies geschieht auf der 802.11-Ebene und wird durch die WPA-Informationselemente in Beacon Frames, Probe Responses und Anforderungen für (erneute) Zuordnung kommuniziert. Zu den in diesen Elementen enthaltenen Informationen gehören die Authentifizierungsmethode (802.1x oder Pre-Shared Key) und die bevorzugte Codierungsart (WEP, TKIP oder AES).

  Die wichtigste Information in den Beacon Frames ist die Authentifizierungsmethode und die Codierungsart. Zu den möglichen Authentifizierungsmethoden gehören 802.1x und Pre-Shared Key. Pre-Shared Key ist eine Authentifzierungsmethode, bei der sowohl für die Stationen als auch für den Access Point ein statisch konfiguriertes Passwort verwendet wird. So ist kein Authentifizierungsserver erforderlich. Dies macht diese Methode besonders interessant für Heimnetzwerke und kleine Büroumgebungen. Zu den anderen Codierungsmöglichkeiten gehören WEP, TKIP und AES (Advanced Encryption Standard). TKIP und AES werden unten im Zusammenhang mit der Datensicherheit näher erläutert

- Authentifizierung. Zur Authentifizierung wird EAP über 802.1x eingesetzt. Die für WPA erforderliche gegenseitige Authentifizierung kann durch einen EAP-Typ, der diese Funktion unterstützt, ermöglicht werden. 802.1x-Port-Zugriffskontrolle gewährt erst dann uneingeschränkten Zugriff auf das Netzwerk, wenn die Authentifizierung abgeschlossen ist. WAP verwendet 802.1x-EAPOL-Schlüsselpakete zur Verteilung von nur für die jeweilige Sitzung gültigen Schlüsseln an die erfolgreich authentifizierten Stationen.

  Der Antragsteller in der Station entscheidet anhand der in den Informationselementen enthaltenen Informationen zur Authentifizierung und Codierungsart, welche Authentifizierungsmethode und Codierung er verwendet. Wenn der Access Point z. B. das Verfahren Pre-Shared Key (PSK) verwendet, ist eine 802.1x-Authentifizierung nicht erforderlich. Es reicht aus, wenn der Antragsteller dem Access Point den richtigen Pre-Shared Key präsentieren kann. Wenn der Antragsteller keine WPA-Informationselemente entdeckt, weiß er, dass er zum Zugriff auf das Netzwerk eine Authentifizierungsmethode und Schlüsselverwaltung verwenden muss, die älter ist als WPA 802.1x.
- Schlüsselverwaltung. WPA/WPA2 beinhaltet ein stabiles System zur Erstellung und Verwaltung von Schlüsseln, in das auch Authentifizierung und Datensicherheit integriert sind. Die Schlüssel werden nach der erfolgreichen Authentifizierung durch einen vierfachen Handshake zwischen Station und Access Point erstellt.
- Datensicherheit (Verschlüsselung). TKIP (Temporal Key Integrity Protocol) wird als Ergänzung von WEP eingesetzt, um dessen Schwächen mit leistungsstarken Verschlüsselungs- und Sicherheitstechniken auszugleichen.
- Datenintegrität. TKIP fügt am Ende jeder Klartextnachricht einen MIC (Message Integrity Code) an, um eine Verfälschung von Nachrichten zu verhindern.

WPA-/WPA2-Authentifizierung: Benutzerauthentifizierung in Unternehmensnetzwerken über 802.1x/EAP und RADIUS

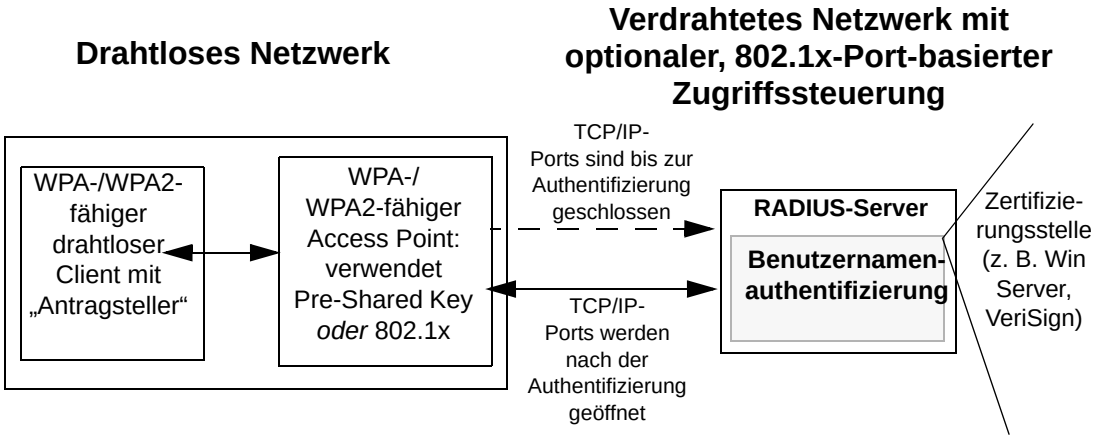

Drahtloses Netzwerk
Verdrahtetes Netzwerk mit optionaler, 802.1x-Port-basierter Zugriffssteuerung
WPA-/WPA2-fähiger drahtloser Client mit „Antragsteller“
WPA-/ WPA2-fähiger Access Point: verwendet Pre-Shared Key *oder* 802.1x
TCP/IP-Ports sind bis zur Authentifizierung geschlossen
TCP/IP-Ports werden nach der Authentifizierung geöffnet
RADIUS-Server
Benutzernamen-authentifizierung
Zertifizierungsstelle (z. B. Win Server, VeriSign)

Abbildung D-3: Übersicht über WPA/WPA2

IEEE 802.1x ist ein effektives Modell für die Authentifizierung und Kontrolle des Benutzerflusses in einem geschützten Netzwerk und stellt darüber hinaus eine Möglichkeit zum dynamischen Wechsel von Datenschlüsseln bereit, z. B über EAP von einem RADIUS-Server. Dieses Modell ermöglicht zudem den Einsatz eines Authentifizierungsservers zur gegenseitigen Authentifizierung. So wird verhindert, dass unerwünschte Benutzer sich Zugang zum drahtlosen Netzwerk verschaffen.

Die eigentlichen Authentifizierungsmechanismen sind jedoch nicht Bestandteil von 802.1x. Bei der Verwendung von 802.1x legt der EAP-Typ (z. B. EAP-TLS (Transport Layer Security) oder EAP-TTLS (EAP Tunneled Transport Layer Security)) fest, wie die Authentifizierung verläuft.

Hinweis: Für Umgebungen mit einer RADIUS-Infrastruktur (Remote Authentication Dial-In User Service) unterstützt WPA EAP (Extensible Authentication Protocol). Für Umgebungen ohne RADIUS-Infrastruktur unterstützt WPA den Einsatz eines Pre-Shared Key.

Zusammengenommen bilden diese Verfahren die Grundstruktur für eine leistungsfähige Benutzerauthentifizierung.

In Windows XP ist 802.1x integriert, und etliche Switches und Wireless Access Points von NETGEAR unterstützen diesen Standard.

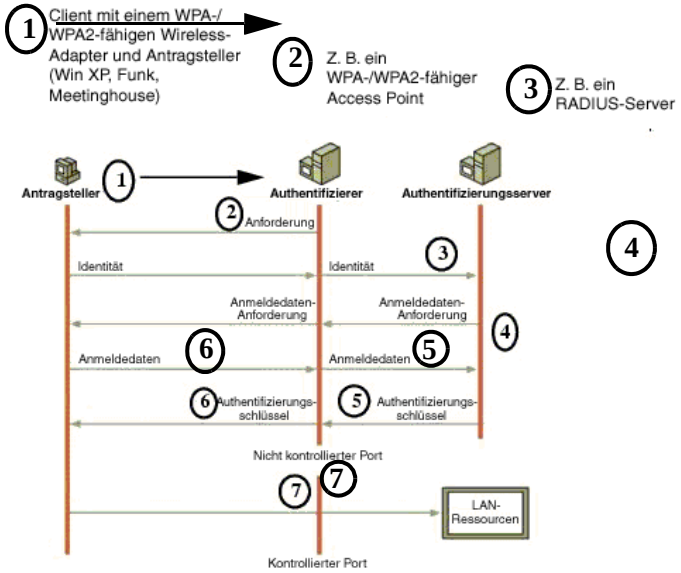


Abbildung D-4: Ablauf der 802.1x-Authentifizierung

Der Access Point sendet Beacon-Frames mit einem WPA-/WPA2-Informationselement an die Stationen im Service Set. Das Informationselement enthält die erforderliche Authentifizierungsmethode (802.1x oder Pre-Shared Key) und die bevorzugte Codierungsart (WEP, TKIP oder AES). Auch Probe Requests (vom Access Point an die Station) und Zuordnungsanforderungen (von der Station zum Access Point) enthalten WPA-Informationselemente.

1. Die einleitende 802.1x-Kommunikation beginnt mit dem Versuch eines nicht authentifizierten Antragstellers (Client), eine Verbindung zu einem Authentifizierer (802.11-Access-Point) aufzubauen. Der Client sendet eine EAP-Startnachricht. Dadurch wird eine Reihe von Nachrichtenwechseln zur Authentifizierung des Clients eingeleitet.
2. Der Access Point antwortet mit einer EAP-Identitätsanforderung.

3. Der Client sendet ein EAP-Antwortpaket mit der Identität an den Authentifizierungsserver. Der Access Point gibt daraufhin einen Port frei, über den der Client ausschließlich EAP-Pakete an den Authentifizierungsserver senden kann. Dieser Port befindet sich auf der verkabelten Seite des Access Points. Der Access Point blockiert alle anderen Arten von Datenverkehr wie HTTP-, DHCP- und POP3-Pakete, bis die Identität des Clients durch einen Authentifizierungsserver (z. B. einen RADIUS-Server) bestätigt wurde.
4. Der Authentifizierungsserver überprüft die Identität des Clients mit Hilfe eines speziellen Authentifizierungsalgorithmus. Dabei können digitale Zertifikate oder andere Arten der EAP-Authentifizierung zum Einsatz kommen.
5. Der Authentifizierungsserver sendet eine Bestätigungs- oder Ablehnungsnachricht an den Access Point.
6. Der Access Point sendet ein EAP-Erfolgspaket (oder Ablehnungspaket) an den Client.
7. Wenn der Authentifizierungsserver den Client akzeptiert, ändert der Access Point den Status des Client-Ports zu autorisiert und leitet zusätzliche Daten weiter.

An dieser Stelle ist zu beachten, dass die Software, die den EAP-Typ unterstützt, auf dem Authentifizierungsserver installiert ist sowie Bestandteil des Betriebssystems bzw. der Antragstellersoftware der Client-Geräte ist. Der Access Point gibt die 802.1x-Nachrichten lediglich weiter. Dies bedeutet, dass Sie einen beliebigen EAP-Typ angeben können, ohne deswegen einen 802.1x-kompatiblen Access Point anschaffen zu müssen. Demzufolge können Sie den EAP-Authentifizierungstyp auch auf Methoden wie Token Cards (Smart Cards), Kerberos, Einmalpasswörter, Zertifikate und öffentliche Schlüssel erweitern. Selbst wenn neue Authentifizierungsmethoden entwickelt werden und Ihre Sicherheitsanforderungen sich ändern, können Sie diese integrieren.

WPA-/WPA2-Schlüsselverwaltung

Bei 802.1x ist die Neuverschlüsselung von Unicast-Schlüsseln optional. 802.11 und 802.1x bieten zudem keinen Mechanismus zum Ändern des globalen Schlüssels für den Multicast- und Broadcast-Datenversand. Bei WPA/WPA2 ist die Neuverschlüsselung sowohl für Unicast-Schlüssel als auch für globale Schlüssel obligatorisch.

Unicast-Schlüssel werden durch das TKIP (Temporal Key Integrity Protocol) für jedes Frame geändert. Die Änderung wird zwischen dem drahtlosen Client und dem Wireless Access Point synchronisiert. Änderungen des globalen Schlüssels können bei WPA mit Hilfe des Informationselements vom Wireless Access Point an die angeschlossenen drahtlosen Clients weitergegeben werden.

802.1x-Authentifizierungsserver, die für einen dynamischen Schlüsselaustausch konfiguriert sind, können dem Access Point gemeinsam mit der Bestätigungsnachricht einen Sitzungsschlüssel übermitteln. Der Access Point kann mit dem Sitzungsschlüssel eine EAP-Schlüsselnachricht erstellen, unterzeichnen und verschlüsseln, die untermittelbar nach der Erfolgsnachricht an den Client gesendet wird. Der Client kann dann anhand der Schlüsselnachricht die erforderlichen Schlüssel definieren. In typischen 802.1x-Implementierungen kann der Client Schlüssel so oft wie nötig automatisch ändern, um das Risiko zu minimieren, dass unerwünschte Eindringlinge genügend Zeit haben, den aktuellen Schlüssel zu knacken.

TKIP (Temporal Key Integrity Protocol)

Mit TKIP verfügt WPA über wichtige Verbesserungen zur Datenverschlüsselung, z. B. eine Funktion zum paketweisen Ändern von Schlüsseln, die Nachrichtenintegritätsprüfung Michael (Message Integrity Check, MIC), einen erweiterten Initialisierungsvektor (IV) mit Sequenzierungsregeln und einen Mechanismus zur Neuverschlüsselung. Darüber hinaus bietet TKIP die folgenden Funktionen:

- Verifizierung der Sicherheitskonfiguration nach Festlegen der Schlüssel
- Synchronisierte Änderung des Unicast-Schlüssels für alle Frames
- Erstellung eines eindeutigen Unicast-Startschlüssels für jede Pre-Shared-Key-Authentifizierung

Michael

Bei 802.11 und WEP wird Datenintegrität über einen 32-Bit-ICV (*Integrity Check Value*) gewährleistet, der an die 802.11-Nutzinformationen angehängt und über WEP verschlüsselt wird. Obwohl der ICV verschlüsselt ist, lassen sich per Kryptoanalyse Teile der verschlüsselten Nutzinformationen ändern und der verschlüsselte ICV aktualisieren, ohne dass der Empfänger dies bemerkt.

Bei WPA legt eine Methode namens *Michael* einen neuen Algorithmus fest, über den die Berechnungsvorrichtungen der drahtlosen Geräte einen 8-Byte-MIC (Message Integrity Check) errechnen. Der MIC wird zwischen dem Datenabschnitt des IEEE 802.11-Frame und dem 4-Byte-ICV platziert. Das MIC-Feld wird zusammen mit den Frame-Daten und dem ICV verschlüsselt.

Michael bietet zudem Wiederholungsschutz. Mit einem neuen Frame-Zähler in IEEE 802.11 können Wiederholungsangriffe verhindert werden.

AES-Unterstützung für WPA2

WPA2 unterstützt unter anderem die Verschlüsselungsmethode AES (Advanced Encryption Standard). AES-Unterstützung wird jedoch zunächst nicht zu den Voraussetzungen für eine Wi-Fi-Zertifizierung gehören. AES gilt als optimale Wahl für sicherheitsbewusste Unternehmen, stellt sie jedoch vor ein Problem: AES erfordert eine grundlegende Neugestaltung der Hardware der Netzwerkschnittstellenkarten der Station und des Access Points. TKIP ist ein pragmatischer Kompromiss, der Unternehmen bessere Sicherheit bietet, während AES-kompatible Geräte entwickelt, hergestellt und nach und nach eingeführt werden.

Sind mit WPA/WPA2 alle Probleme gelöst?

Auch WPA/WPA2 hat seine Schwächen. Es ist besonders anfällig für Denial-of-Service-Angriffe. Wenn der Access Point innerhalb von 60 Sekunden zwei Datenpakete empfängt, die nicht über den erforderlichen MIC (Message Integrity Code) verfügen, steht das Netzwerk unter Angriff. Dies führt dazu, dass der Access Point Gegenmaßnahmen einleitet, darunter auch die Unterbrechung der Verbindung zu allen Stationen, die den Access Point verwenden. Dies verhindert, dass Angreifer sich Informationen über den Schlüssel verschaffen, und macht zudem die Administratoren auf das Problem aufmerksam. Es bedeutet jedoch leider auch, dass Benutzer für 60 Sekunden die Verbindung zum Netzwerk verlieren. Vor allem aber beweist es, dass keine einzelne Sicherheitstaktik vollkommenen Schutz gewährleisten kann. WPA/WPA2 bedeutet gegenüber WEP definitiv einen großen Fortschritt der WLAN-Sicherheit. Es sollte jedoch als eine Komponente einer umfassenden Netzwerksicherheitsstrategie betrachtet werden.

Produktunterstützung für WPA/WPA2

Seit August 2003 unterstützen drahtlose Produkte von NETGEAR, Inc. mit Wi-Fi-Zertifizierung den WPA-Standard. Drahtlose Produkte von NETGEAR, Inc., deren Wi-Fi-Zertifizierung vor August 2003 erteilt wurde, hatten ein Jahr Zeit, um WPA hinzuzufügen und so ihre Wi-Fi-Zertifizierung zu behalten.

Für WPA/WPA2 sind Software-Änderungen in den folgenden Bereichen erforderlich:

- Wireless Access Points
- Drahtlose Netzwerkadapter
- Programme für drahtlose Clients

Änderungen an Wireless Access Points

Die Firmware von Wireless Access Points muss aktualisiert werden, um die folgenden Funktionen zu unterstützen:

- **Das neue WPA-/WPA2-Informationselement**
  Wireless Access Points signalisieren, dass sie WPA/WPA2 unterstützen, indem sie das Beacon-Frame mit einem neuen 802.11-WPA-/WPA2-Informationselement, das die Sicherheitskonfiguration des Wireless Access Points (Verschlüsselungsalgorithmen und Informationen über die Konfiguration der drahtlosen Sicherheit) enthält, versenden.
- **Die WPA-/WPA2-Zwei-Phasen-Authentifizierung**
  Open System, dann 802.1x (EAP mit RADIUS oder Pre-Shared Key).
- **TKIP**
- **Michael**
- **AES** (WPA2)

Um ältere Wireless Access Points zur Unterstützung von WPA/WPA2 aufzurüsten, müssen Sie sich vom Anbieter der Wireless Access Points ein WPA-/WPA2-Firmware-Update besorgen und dieses auf den Wireless Access Points installieren.

Änderungen an drahtlosen Netzwerkadaptern

Die WLAN-Software im Adapter (und möglicherweise auch im Betriebssystem oder der Client-Anwendung) muss aktualisiert werden, um die folgenden Funktionen zu unterstützen:

- **Das neue WPA-/WPA2-Informationselement**
  Drahtlose Clients müssen in der Lage sein, das WPA-/WPA2-Informationselement zu verarbeiten und darauf mit einer spezifischen Sicherheitskonfiguration zu reagieren.
- **Die WPA-/WPA2-Zwei-Phasen-Authentifizierung**
  Open System, dann 802.1x-Antragsteller (EAP oder Pre-Shared Key).
- **TKIP**
- **Michael**
- **AES** (WPA2)

Um Ihre drahtlosen Netzwerkkarten zur Unterstützung von WPA/WPA2 aufzurüsten, müssen Sie sich gegebenenfalls vom Anbieter der drahtlosen Netzwerkkarten ein WPA-/WPA2-Firmware-Update besorgen und damit die Treiber der drahtlosen Netzwerkkarten aktualisieren.

Bei drahtlosen Windows-Clients müssen Sie sich einen aktualisierten Netzwerktreiber besorgen, der WPA unterstützt. Treiber für drahtlose Netzwerkkarten, die mit Windows XP (Service Pack 1) und Windows Server 2003 kompatibel sind, müssen nach der Aktualisierung in der Lage sein, die WPA-Fähigkeit und die Sicherheitskonfiguration der Karte an den „Wireless Zero Configuration“-Dienst zu übermitteln.

Microsoft hat mit zahlreichen Anbietern drahtloser Geräte zusammengearbeitet, um das WPA-Treiber-Update in den Treiber für drahtlose Netzwerkkarten zu integrieren. Zur Aktualisierung eines drahtlosen Windows-Clients müssen Sie sich also lediglich den neuen WPA-/WPA2-kompatiblen Treiber besorgen und diesen installieren.

Änderungen an Programmen für drahtlose Clients

Die Programme für drahtlose Clients müssen aktualisiert werden, um die Konfiguration der WPA-/WPA2-Authentifizierung (sowie von Pre-Shared-Key) und die Unterstützung der neuen WPA-/WPA2-Verschlüsselungsalgorithmen (TKIP und AES) zu ermöglichen.

Microsofts WPA-Clientprogramm ist über die Website von Microsoft erhältlich.

Hinweis: Microsofts WPA2-Client befindet sich noch in der Beta-Phase.

Glossar

Dieses Glossar enthält Definitionen der Fachausdrücke, die in diesem Handbuch verwendet werden.

802.11 (Standard)

802.11 bzw. IEEE 802.11 ist eine Funktechnik, die in drahtlosen LANs (Wireless Local Area Networks, WLANs) eingesetzt wird. Es handelt sich dabei um einen Standard, der vom IEEE (Institute of Electrical and Electronic Engineers, *http://standards.ieee.org*) entwickelt wurde. Das IEEE ist eine internationale Organisation, die Standards für Hunderte von elektronischen und elektrischen Geräten entwickelt. Die Organisation verwendet zur Unterscheidung der unterschiedlichen Technologiefamilien Zahlen (ähnlich wie die Dewey-Dezimalklassifikation in Bibliotheken).

Die Untergruppe 802 (der IEEE) entwickelt Standards für LANs und WANs. Die Abteilung 802.11 ist dabei für die Überprüfung und Entwicklung von Standards für drahtlose LANs (WLANs) zuständig.

WiFi, 802.11, setzt sich aus mehreren Standards zusammen, die für unterschiedliche Frequenzen gelten: 802.11b ist der Standard für WLANs im 2,4-GHz-Spektrum mit einer Bandbreite von 11 MBit/s; 802.11a ist ein anderer WLAN-Standard und gehört zu Systemen, die im Frequenzbereich 5 GHz mit einer Bandbreite von 54 MBit/s arbeiten. Der Standard 802.11g gilt für WLANs, die im Frequenzbereich 2,4 GHz mit einer Bandbreite von 54 MBit/s arbeiten.

802.11a (Standard)

Ein IEEE-Standard für drahtlose Netzwerke im Frequenzbereich 5 GHz (5,15 GHz bis 5,85 GHz) mit einer maximalen Datenübertragungsrate von 54 MBit/s. Der 5-GHz-Frequenzbereich ist nicht so überfüllt wie der 2,4-GHz-Bereich, da der Standard 802.11a mehr Funkkanäle bietet als Standard 802.11b. Diese zusätzlichen Kanäle können helfen, Radio- und Mikrowellenstörungen zu vermeiden.

802.11b (Standard)

Ein internationaler Standard für drahtlose Netzwerke im Frequenzbereich 2,4 GHz (2,4 GHz bis 2,4835 GHz) mit einem Datendurchsatz von bis zu 11 MBit/s. Dieser Frequenzbereich wird sehr stark genutzt. Mikrowellengeräte, schnurlose Telefone, medizinische und wissenschaftliche Geräte sowie Bluetooth-Geräte verwenden allesamt das 2,4-GHz-Frequenzband.

802.11d (Standard)

802.11d ist eine Ergänzung des IEEE-Standards 802.11 zur MAC-Schicht (Media Access Control), die die weltweite Nutzung von 802.11-WLANs fördern soll. Dabei wird Access Points die Übermittlung von Daten über die zulässigen Funkkanäle mit akzeptabler Leistungsstärke für die Client-Geräte ermöglicht. Die Geräte werden dabei automatisch an die geografischen Anforderungen angepasst.

Der Standard 802.11d soll Funktionen und Einschränkungen festlegen, die den Betrieb von WLANs in den entsprechenden Ländern ermöglichen. Gerätehersteller möchten keine Vielzahl landesspezifischer Produkte herstellen und Benutzer, die viel reisen, möchten nicht für jedes Land eine eigene WLAN-PC-Card anschaffen. Dies wird langfristig zu landesspezifischen Firmware-Lösungen führen.

802.11e (Standard)

802.11e ist ein geplanter IEEE-Standard zur Definition von QoS-Mechanismen (Quality of Service) für drahtlose Geräte, der bandbreitenempfindliche Anwendungen wie Telefon und Video unterstützt.

802.11g (Standard)

Dieser Standard zur Erweiterung der Bitübertragungsschicht ist 802.11b sehr ähnlich, erlaubt jedoch einen Datendurchsatz von bis zu 54 MBit/s. Dieser Standard verwendet das 2,4-GHz-Frequenzband, setzt jedoch eine andere Funktechnik ein, um die Gesamtbandbreite zu vergrößern.

802.11i

Dieser Name bezeichnet die IEEE-Arbeitsgruppe, die sich mit der Standardisierung der WLAN-Sicherheit befasst. Das Sicherheitsrahmenwerk von 802.11i basiert auf RSN (Robust Security Network). RSN setzt sich aus zwei Teilen zusammen: 1.) Einem Datensicherheitsmechanismus und 2.) Verwaltung der Sicherheitsbeziehungen (Security Association Management).

Der Datensicherheitsmechanismus unterstützt zwei geplante Verschlüsselungsmethoden: TKIP and AES. TKIP (Temporal Key Integrity Protocol) ist eine Übergangslösung, die Software-Patches für WEP definiert, damit ein Mindestmaß an Datensicherheit gewährleistet ist. AES oder AES-OCB (Advanced Encryption Standard & Offset Codebook) ist ein leistungsstarkes Datensicherheitsschema, das als langfristige Lösung gedacht ist.

Die Verwaltung der Sicherheitsbeziehungen wird über drei Verfahren geregelt: a.) RSN-Abstimmungsverfahren, b.) IEEE-802.1x-Authentifizierung und c.) IEEE-802.1x-Schlüsselverwaltung.

Die Standards wurden so definiert, dass sie eine Koexistenz mit derzeit implementierten Netzwerken, die noch aus der Zeit vor RSN stammen, ermöglichen.

802.11n (Standard)

Eine im Oktober 2003 gebildete Arbeitsgruppe der IEEE, die als „802.11n“ oder „TGn“ bezeichnet wird. Sie ist zuständig für das 100 MBit/s-Standardprotokoll in der Bitübertragungsschicht. Als Veröffentlichungstermin ist derzeit Dezember 2005 geplant. Im Februar 2004 war noch kein Entwurf verfügbar. Es wird jedoch erwartet, dass das Protokoll sowohl die 2,4- als auch die 5-GHz-Frequenz verwendet.

Ad-hoc-Modus

Eine Client-Einstellung, die unabhängige Peer-to-Peer-Verbindungen über ein WLAN ermöglicht. Eine andere Einsatzmöglichkeit ist die Kommunikation von PCs untereinander über einen Access Point. Siehe Access Point und Infrastruktur-Modus.

Access Point (auch Zugangspunkt)

Ein WLAN-Sende-/Empfangsgerät (oft auch als „Basisstation“ bezeichnet), über das ein oder mehrere drahtlose Geräte an ein kabelgebundenes LAN angeschlossen werden können. Über eine Funkbrücke können Access Points auch miteinander kommunizieren.

Es gibt unterschiedliche Typen von Access Points (Basisstationen), die sowohl in drahtlosen als auch in kabelgebundenen Netzwerken eingesetzt werden. Dazu gehören Bridges, Hubs, Switches, Router und Gateways. Die Unterschiede zwischen diesen Geräten sind nicht immer klar definiert, da bestimmte Funktionen, die einem dieser Geräte zugeordnet werden, auch in andere Geräte integriert werden können. So kann z. B. ein Router Funktionen einer Bridge übernehmen oder ein Hub auch als Switch eingesetzt werden. Alle diese Geräte dienen jedoch dazu, Daten von einem Ort an einen anderen zu übertragen.

Eine Bridge verbindet Geräte, die dasselbe Protokoll verwenden. Über einen Router können Netzwerke verbunden werden, in denen unterschiedliche Protokolle zum Einsatz kommen. Der Router liest zudem die in den Paketen enthaltenen Adressen und leitet die Pakete an die entsprechende Computerstation weiter. Dabei arbeitet er mit den anderen Routern im Netzwerk zusammen, um den besten Pfad zum Versand der Pakete zu finden. Ein drahtloser Hub oder Access Point verfügt neben anderen zusätzlichen Funktionen über Roaming und bietet eine Netzwerkverbindung zu einer Vielzahl von Clients. Er vergibt jedoch keine Bandbreite. Ein Switch ist ein Hub mit besonderen Fähigkeiten: Er kann die Adresse auf einem Paket lesen und dieses an die entsprechende Computerstation weiterleiten. Bei einem Wireless Gateway handelt es sich um einen Access Point, der zusätzliche Funktionen, wie NAT-Routing, DHCP, Firewalls und Sicherheit, bereitstellt.

AES (Advanced Encryption Standard)

Ein 128-Bit-Block-Datenverschlüsselungsverfahren, das von den belgischen Kryptographieexperten Joan Daemen und Vincent Rijmen entwickelt wurde. Die Regierung der Vereinigten Staaten übernahm im Oktober 2000 diesen Algorithmus als Verschlüsselungsverfahren anstelle der bisher verwendeten DES-Verschlüsselung. AES operiert auf mehreren Netzwerkschichten zugleich. Das National Institute of Standards and Technology (NIST) des US-Handelsministeriums wählte den Algorithmus „Rijndael“ aus einer Gruppe von fünf in die nähere Auswahl genommenen Algorithmen, darunter auch ein Algorithmus namens „MARS“ von einem großen Entwicklungsteam bei IBM. AES wird WEP voraussichtlich 2006 als WLAN-Verschlüsselungsmethode ablösen.

Bandbreite

Die Übertragungskapazität, die in einem Netzwerk zur Verfügung steht. Die verfügbare Bandbreite hängt von mehreren Variablen ab, darunter die Datenübertragungsrate zwischen Geräten im Netzwerk, der Netzwerk-Overhead, die Benutzeranzahl und der Typ des Geräts, über das PCs an das Netzwerk angeschlossen werden. Die Bandbreite lässt sich gewissermaßen mit einem Rohr vergleichen, da bei beiden die Größe die Kapazität bestimmt: Je breiter das Rohr ist, desto mehr Wasser kann hindurchfließen, und je mehr Bandbreite ein Netzwerk zur Verfügung stellt, desto mehr Daten können hindurchfließen. Der Standard 802.11b bietet eine Bandbreite von 11 MBit/s; 802.11a und 802.11g dagegen 54 MBit/s.

Bit pro Sekunde (Bit/s)

Maßeinheit für die Datenübertragungsgeschwindigkeit über Kommunikationsleitungen, basierend auf der Anzahl von Bit, die pro Sekunde versendet oder empfangen werden können. Bit pro Sekunde (Bit/s) werden oft mit Bytes pro Sekunde (Bytes/s) verwechselt. Während Bits zum Messen der Übertragungsgeschwindigkeit verwendet werden, dienen Bytes zur Angabe der Speicherkapazität. 8 Bits ergeben ein Byte. Wenn ein drahtloses Netzwerk also mit einer Bandbreite von 11 Megabits pro Sekunde (11 MBit/s) arbeitet, versendet es pro Sekunde 1,375 Megabytes (1,375 Mbytes/s).

Bluetooth-Funktechnik

Eine technische Spezifikation zum Verbinden von tragbaren Computern, PDAs und Mobiltelefonen für die drahtlose Übertragung von Telefongesprächen und Daten über kurze Entfernungen mit Hilfe eines globalen Funkfrequenzbands. Bluetooth ist ein Frequenzsprungverfahren im Frequenzspektrum 2,4 GHz mit einer Reichweite von bis zu zehn Metern und einem Datendurchsatz von bis zu 1 MBit/s.

Bridge

Ein Gerät zum Verbinden eines LANs (Local Area Network) mit einem anderen LAN, das dasselbe Protokoll verwendet (z. B. drahtlos, Ethernet oder Token Ring). Wireless Bridges werden sehr häufig eingesetzt, um die unterschiedlichen Gebäude auf einem Universitätscampus zu verbinden.

Clients oder Client-Geräte

Jeder Computer in einem Netzwerk, der Dienste (Dateien, Druckfunktionen) von einem anderen Mitglied des Netzwerks bezieht. Clients sind Endbenutzer. Zu den WiFi-Client-Geräten gehören PC Cards für Notebook-Computer, Mini-PCI-Module in Notebook-Computern und mobilen Geräten sowie USB- und PCI-/ISA-Bus-WiFi-Radios. Client-Geräte kommunizieren in der Regel mit Hub-Geräten wie Access Points und Gateways.

Crossover-Kabel

Ein spezielles Kabel, mit dem zwei Computer ohne einen Hub vernetzt werden können. Crossover-Kabel werden zudem manchmal benötigt, um ein Kabel- oder DSL-Modem mit einem Wireless Gateway oder Access Point zu verbinden. Die Signale werden nicht parallel von einem Stecker zum nächsten geführt, sondern „gekreuzt“. Wird zum Beispiel ein Kabel mit acht Leitungen verwendet, geht das Signal am einen Ende des Kabels über Pin 1 ein und kommt am anderen Ende auf Pin 8 an. Die Signale wechseln von einer Seite auf die andere.

CSMA/CA (Carrier Sense Multiple Action/Collision Avoidance)

CSMA/CA ist die Hauptmethode für den Zugriff auf Medien in IEEE-802.11-WLANs. Diese Methode folgt dem Prinzip „Erst zuhören, dann reden“ und verringert die Anzahl von Kollisionen, die durch gleichzeitigen Datenversand verursacht werden. Ganz verhindert werden diese Kollisionen dadurch allerdings nicht. IEEE 802.11 legt fest, dass die Kollisionsvermeidungsmethode (und nicht Kollisionserkennung (Collision Detection)) verwendet werden soll, da der Standard Halbduplexbetrieb zu Grunde legt – d. h. es kann nur entweder gesendet oder empfangen werden, aber nicht beides gleichzeitig.

Im Gegensatz zu konventionellen, kabelgebundenen Hosts kann eine WLAN-Station eine Kollision während des Sendens nicht erkennen. Wenn es zu einer Kollision kommt, erhält die Sendestation kein ACK-Paket (ACKnowledge) von der Empfängerstation. Aus diesem Grund haben ACK-Pakete die höchste Priorität im Netzwerk. Nach Abschluss einer Datenübertragung beginnt die Empfangsstation mit dem Senden des ACK-Pakets, bevor ein anderer Knoten den Versand eines neuen Datenpakets einleiten kann. Alle anderen Stationen müssen eine längere pseudo-zufällige Zeitspanne warten, bevor sie senden können. Wenn die Sendestation kein ACK-Paket erhält, wartet sie die nächste Gelegenheit für einen erneuten Übertragungsversuch ab.

CSMA/CD (Carrier Sense Multiple Action/Collision Detection)

Eine Methode zum Verwalten des Datenverkehrs und Verringern von Rauschen in kabelgebundenen Netzwerken. Ein Netzwerkgerät überträgt Daten, nachdem es einen verfügbaren Kanal entdeckt hat. Wenn jedoch zwei Geräte gleichzeitig Daten senden, entdecken die sendenden Geräte eine Kollision und senden die Daten nach Ablauf eines zufälligen Zeitraums erneut.

DHCP (Dynamic Host Configuration Protocol)

Ein Dienstprogramm, das Servern das dynamische Zuweisen von IP-Adressen aus einer vordefinierten Liste ermöglicht. Die Server können zudem die Nutzungszeit der Adressen begrenzen, damit diese erneut vergeben werden können. Ohne DHCP müssten IT-Administratoren die IP-Adressen auf allen Computern im gesamten Netzwerk manuell eingeben. Unter Verwendung von DHCP wird jedem Computer bei der Anmeldung beim Netzwerk automatisch eine IP-Adresse zugewiesen.

Diversity-Antennen

Ein Antennensystem, das zwei Antennen einsetzt, um Empfangs- und Übertragungsqualität zu optimieren und Störungen zu minimieren.

DNS (Domain Name Service)

Ein Programm, das mit Hilfe einer auf mehreren Internetservern gespeicherten Datenbank URLs in IP-Adressen umwandelt. Das Programm läuft im Hintergrund und erleichtert das Surfen im Internet, da so statt numerischer alphabetische Adressen eingesetzt werden können. Ein DNS-Server wandelt einen Namen wie „mywebsite.com“ in eine Zahlenfolge wie „107.22.55.26“ um. Jede Website im Internet hat ihre eigene spezifische IP-Adresse.

Drahtloses Netzwerk

Die Infrastruktur, die die drahtlose Übertragung von Signalen ermöglicht, wird als drahtloses Netzwerk bezeichnet. In einem Netzwerk sind unterschiedliche Geräte miteinander verbunden, und Ressourcen können von mehreren Teilnehmern gemeinsam genutzt werden.

ESSID (häufig auch als „SSID“ – Service Set Identifier – bezeichnet)

Die Kennung eines drahtlosen 802.11-Netzwerks. Durch Angabe der richtigen ESSID beim Einrichten des Clients melden Sie sich bei Ihrem drahtlosen Netzwerk an (statt bei einem anderen Netzwerk in Reichweite). (Siehe SSID.) Andere Bezeichnungen für die ESSID sind Netzwerkname, bevorzugtes Netzwerk, SSID oder Wireless LAN Service Area.

Ethernet

Internationaler Standard (Übertragungsprotokoll) für kabelgebundene Netzwerke. Einfache 10BaseT-Netzwerke bieten eine Bandbreite von ca. 10 MBit/s. Fast Ethernet (100 MBit/s) und Gigabit Ethernet (1000 MBit/s) werden immer beliebter.

Firewall

Ein System, das Netzwerke schützt und den Zugriff durch Unbefugte verhindert. Firewalls sind in Form von Software, Hardware oder einer Kombination aus beiden erhältlich. Firewalls können den Zugang zu einem Netzwerk regulieren sowie den Datenfluss nach außen einschränken.

Gateway

Üblicherweise ein Gerät, das eine Verbindung zu einem anderen Netzwerk, z. B. dem Internet, herstellt. Gateways können zudem VPN-Unterstützung, Firewalls, unterschiedliche Sicherheitsstufen und Wireless Access Points mit weiteren Funktionen beinhalten.

Hot-Spot

Hot-Spots bieten Zugang zu WiFi-Diensten. Dies kann kostenlos oder gebührenpflichtig sein. Hot-Spots sind in Cafés, Flughäfen, Bahnhöfen, Kongresszentren, Hotels und an anderen öffentlichen Orten zu finden. Unternehmen und Hochschulen richten ebenfalls Hot-Spots ein, um Besuchern und Gästen die Möglichkeit zum drahtlosen Internetzugang zu bieten. In manchen Ländern werden Hot-Spots als „Coolspots“ bezeichnet.

Hub

Ein Gerät mit mehreren Ports, über das PCs per Netzwerkkabel oder WiFi an ein Netzwerk angeschlossen werden können. Kabelgebundene Hubs können zahlreiche Ports haben und die Übertragungsgeschwindigkeit kann von 10 MBit/s bis zu mehreren Gigabyte pro Sekunde reichen. Ein Hub sendet die Pakete, die er empfängt, an alle angeschlossenen Ports. An einen kleinen kabelgebundenen Hub können nur 4 Computer angeschlossenen werden, an einen großen Hub 48 und mehr. An drahtlose Hubs (Access Points) können sogar Hunderte von Computern angeschlossen werden.

Hz (Hertz)

Die SI-Einheit für die Frequenz gibt die Anzahl der Schwingungen pro Sekunde an. Ein Megahertz (MHz) entspricht einer Million Hertz, ein Gigahertz (GHz) einer Milliarde Hertz. In den USA ist die Standardstromfrequenz 60 Hz, das Frequenzband für MW-Funk ist 535–1605 kHz, das Frequenzband für UKW-Funk ist 88–108 MHz und 802.11b-WLANs arbeiten bei 2,4 GHz.

IEEE (Institute of Electrical and Electronics Engineers)

Ein Berufsverband, zu dessen Mitgliedern Ingenieure, Wissenschaftler und Studenten der Elektrotechnik und verwandter Fachgebiete gehören (Website: *www.ieee.org*). Das IEEE hat über 300.000 Mitglieder und spielt eine wichtige Rolle bei der Entwicklung von Standards für Computer und Kommunikationstechnik.

IEEE 802.11

Eine Normenfamilie für LANs, herausgegeben vom IEEE (Institute of Electrical and Electronics Engineers). Die meisten kabelgebundenen Netzwerke entsprechen 802.3, dem Standard für CSMA/CD-basierte Ethernetnetzwerke, oder 802.5, dem Standard für Token-Ring-Netzwerke. 802.11 legt den Standard für drahtlose LANs (WLANs) fest und umfasst drei nicht miteinander kompatible Verfahren: FHSS (Frequency Hopping Spread Spectrum), DSSS (Direct Sequence Spread Spectrum) und Infrarot. Die WECA (Wireless Ethernet Compatibility Alliance, inzwischen Wi-Fi Alliance) konzentriert sich auf 802.11b, einen DSSS-Standard für drahtlose Netzwerke mit einer Übertragungsrate von 11 MBit/s.

Infrastruktur-Modus

Eine Client-Einstellung, die Verbindungen zu einem Access Point möglich macht. Im Gegensatz zum Ad-hoc-Modus, in dem PCs direkt miteinander kommunizieren, gehen im Infrastruktur-Modus alle von den Clients versendeten und empfangenen Daten durch einen Access Point. Der Access Point ist nicht nur für

den drahtlosen Netzwerkdatenverkehr in der unmittelbaren Umgebung zuständig, sondern sorgt auch für die Kommunikation mit dem kabelgebundenen Netzwerk. Siehe Ad-hoc-Modus und Access Point.

IP-Adresse (Internet Protocol Address)

Eine 32-Bit-Nummer, die den Sender oder Empfänger jeglicher über das Internet versendeter Daten kennzeichnet. IP-Adressen setzen sich aus zwei Teilen zusammen: Der eine verweist auf ein bestimmtes Netzwerk innerhalb des Internets, der andere verweist auf das jeweilige Gerät (das ein Server oder eine Workstation sein kann) innerhalb dieses Netzwerks.

ISO-OSI-Referenzmodell

Ein von der ISO (International Standards Organization) entwickeltes Netzwerkmodell, das aus sieben Stufen oder Schichten besteht. Durch die Standardisierung dieser Schichten und der Schnittstellen zwischen ihnen können unterschiedliche Elemente eines bestehenden Protokolls angepasst oder geändert werden, um dem technischen Fortschritt und veränderten Systemanforderungen gerecht zu werden. Die sieben Schichten werden wie folgt bezeichnet:

- Bitübertragungsschicht (auch physikalische Schicht, engl. Physical Layer)
- Sicherungsschicht (auch Verbindungssicherungsschicht, Verbindungsebene, Prozedurebene, engl. Data Link Layer)
- Vermittlungsschicht (auch Paketebene, engl. Network Layer)
- Transportschicht (auch Ende-zu-Ende-Kontrolle, Transport-Kontrolle, engl. Transport Layer)
- Kommunikationsschicht (auch Kommunikationssteuerungsschicht, Steuerung logischer Verbindungen, Sitzungsschicht, engl. Session Layer)
- Darstellungsschicht (auch Datendarstellungsschicht, Datenbereitstellungsebene, engl. Presentation Layer)
- Anwendungsschicht (auch Anwenderebene, Verarbeitungsschicht, engl. Application Layer)

Der Standard IEEE 802.11 bezieht sich auf die Bitübertragungsschicht (physikalische Schicht, PHY) und den unteren Bereich der Sicherungsschicht. Der untere Bereich der Sicherungsschicht wird oft als MAC-Schicht (Media Access Control) bezeichnet.

Kollisionsvermeidung (Collision Avoidance)

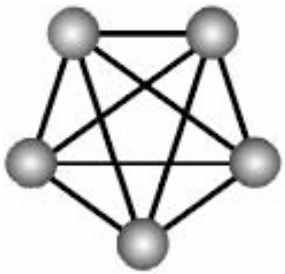
Ein Netzwerkknotenmerkmal für die proaktive Entdeckung, ob ein Signal gesendet werden kann, ohne dabei eine Kollision zu riskieren.

MAC (Media Access Control)

Jedes drahtlose 802.11-Gerät hat seine eigene, unveränderbare MAC-Adresse. Diese eindeutige Kennzeichnung kann genutzt werden, um drahtlose Netzwerke sicherer zu machen. Wenn ein Netzwerk eine MAC-Tabelle einsetzt, erhalten nur diejenigen 802.11-Geräte, deren MAC-Adresse in der MAC-Tabelle dieses Netzwerks aufgelistet sind, Zugang zum Netzwerk.

Maschennetze

Maschennetze (oft auch als „Maschenstruktur“ bezeichnet) sind eine Netzwerktopologie, bei der Geräte über eine Vielzahl von Verbindungen zwischen den einzelnen Netzwerkknoten verbunden werden. In einer vollständigen Mesh Topologie ist jeder Knoten mit allen anderen Knoten im Netzwerk verbunden. Maschennetze können drahtlos oder kabelgebunden sein.



In der oben dargestellten Maschenstruktur entspricht jede Kugel einem Router. Server und Drucker können gemeinsam genutzt werden, indem sie mit jedem Router in der Masche verbunden werden. Für einen drahtlosen Zugang zum Maschennetz muss ein Access Point an einen der Router in diesem Netz angeschlossen werden.

MIMO (Multiple Input Multiple Output)

MIMO bezeichnet Funktechnologien, die zur Optimierung der drahtlosen Kommunikation mit mehreren Verbindungen zwischen Sender und Empfänger arbeiten. Hierzu werden mehrere Antennen benötigt.

NAT (Network Address Translation, Netzwerk-Adressumsetzung)

Eine Netzwerkfunktion, mit der mehrere Computer eine einzige Eingangs-IP-Adresse dynamisch zum gemeinsamen Zugriff auf das Internet über eine Einwähl-, Kabel- oder xDSL-Verbindung nutzen können. NAT verwendet die gemeinsame IP-Adresse und erstellt neue IP-Adressen für alle Client-Computer im Netzwerk.

Netzwerkname

Der Netzwerkname kennzeichnet das drahtlose Netzwerk für alle gemeinsam genutzten Geräte. Bei der Installation eines drahtlosen Netzwerks muss in der Regel ein Netzwerkname bzw. eine SSID eingegeben werden. Beim Einrichten eines einzelnen Computers, eines kabelgebundenen Netzwerks oder einer Arbeitsgruppe werden andere Netzwerknamen verwendet.

Netzwerkkarte (NIC, Network Interface Card)

Eine Steckkarte für PCs, die entweder drahtlos funktioniert oder über einen Anschluss für ein Netzwerkkabel verfügt. In beiden Fällen kann über die Karte eine bidirektionale Kommunikation zwischen dem Computer und Netzwerkgeräten wie einem Hub oder Switch hergestellt werden. Die meisten Netzwerkkarten in kabelgebundenen Büronetzwerken arbeiten mit 10 MBit/s (Ethernet), 100 MBit/s (Fast Ethernet) oder 10/100 MBit/s (Dual Speed). Daneben sind aber auch besonders schnelle Gigabit- und 10-Gigabit-Netzwerkkarten erhältlich. Oft werden Netzwerkkarten auch als Netzwerk-Adapter bezeichnet.

PC-Card

Oberbegriff für scheckkartengroße Erweiterungskarten in 16-Bit- (PCMCIA-) oder 32-Bit- (CardBus-) Technologie. PC-Cards werden vor allem in Notebooks eingesetzt. Zu den als PC-Cards erhältlichen Peripheriegeräten gehören u. a. WiFi-Karten, Speicherkarten, Modems, Netzwerkkarten und Festplatten.

PCI

PCI ist ein leistungsstarker E/A-Bus, mit dem die meisten Computer ausgestattet sind. Andere Bussysteme sind ISA und AGP. PCI und andere Busse ermöglichen den Einbau von internen Karten, die Dienste und Funktionen bieten, die von der Hauptplatine oder anderen Anschlüssen nicht unterstützt werden.

Peer-to-Peer-Netzwerk (bei WLANs auch Ad-hoc-Modus)

Ein kabelgebundenes oder drahtloses Computernetzwerk ohne Server, zentralen Hub oder Router. Alle vernetzten PCs können gleichrangig als Netzwerkserver oder Client agieren und jeder Client-Computer kann mit allen anderen drahtlosen Computern kommunizieren, ohne dabei über einen Access Point oder Hub gehen zu müssen. Da es keine zentrale Basisstation gibt, die den Datenverkehr überwacht oder den Internetzugang zur Verfügung stellt, kann es jedoch zu Kollisionen der einzelnen Signale und damit zu einer Beeinträchtigung der Leistung des Netzwerkes insgesamt kommen.

PHY (physikalische Schicht oder auch Bitübertragungsschicht)

Die unterste Schicht des ISO-OSI-Referenzmodells. Diese Schicht ist in erster Linie für die Übertragung der Bitströme über das PHYsikalische Übertragungsmedium zuständig. Bei drahtlosen Netzwerken ist das Übertragungsmedium der freie Raum. In der Bitübertragungsschicht werden Parameter wie Datenübertragungsrate, Modulationsmethode, Signalparameter, Sender-/Empfängersynchronisierung usw. festgelegt. In einer Funkimplementierung entspricht die Bitübertragungsschicht den Bereichen Funk-Front-End und Basisbandsignalverarbeitung.

Plug & Play

Eine Computersystemfunktion, die die automatische Konfiguration von Zusatz- und Peripheriegeräten wie PC-Cards, Druckern, Scannern und Multimediageräten ermöglicht.

Proxy-Server

Proxy-Server werden in größeren Unternehmen eingesetzt, um den Netzwerkbetrieb und die Sicherheit zu optimieren. Ein Proxy-Server kann die direkte Kommunikation zwischen zwei oder mehr Netzwerken verhindern. Der Proxy-Server leitet zulässige Datenanforderungen an entfernte Server weiter und/oder bearbeitet Datenanfragen direkt mit Hilfe von Daten auf entfernten Servern.

Reichweite

Die Entfernung, die ein drahtloses Netzwerk von einem Access Point aus abdecken kann. Die meisten WiFi-Systeme bieten eine Reichweite von 30 m oder mehr. Je nach Umgebung und der verwendeten Antenne können WiFi-Signale eine Reichweite von bis zu 1,6 km erreichen.

Residential Gateway (Heim-Gateway)

Ein drahtloses Gerät, über das in einem Heimnetzwerk mehrere PCs mit Peripheriegeräten und dem Internet verbunden werden können. Die meisten WiFi-Residential-Gateways bieten zudem auch DHCP und NAT.

RJ-45

Die Standardstecker in kabelgebundenen Netzwerken. RJ-45-Stecker sehen RJ-11-Telefonsteckern sehr ähnlich. RJ-45 können jedoch bis zu acht Leitungen haben, Telefonstecker haben dagegen nur vier.

Roaming

Der nahtlose Wechsel von der Funkzelle eines Access Points in die des nächsten mit einem Notebook oder Desktop-PC, ohne dass dabei die Verbindung unterbrochen wird.

Rogue Access Point

Als „Rogue Access Point“ bezeichnet man einen nicht autorisierten Access Point, der mit dem Heim- oder Unternehmensnetzwerk verbunden ist oder im Stand-Alone-Modus arbeitet (z. B. von einem Parkplatz oder benachbarten Gebäude aus). Rogue Access Points werden nicht von den Netzwerk-Administratoren verwaltet und erfüllen auch nicht die Sicherheitsrichtlinien des Netzwerks. Sie stellen ein beträchtliches Sicherheitsrisiko dar. Es ist zu empfehlen, ein WLAN-System einzusetzen, das das Hinzufügen von Rogue Access Points zu einem bestehenden WLAN so schwer wie möglich macht.

Router

Ein Gerät, das Datenpakete von einem LAN (Local Area Network) oder WAN (Wide Area Network) an ein anderes weiterleitet. Mit Hilfe von Routingtabellen und Routingprotokollen kann der Router die Netzwerkadresse jedes gesendeten Frames entziffern und entscheiden, welche die effizienteste Route für die Weiterleitung des Frames ist. Er berücksichtigt dabei u. a. die Auslastung, Leitungskosten, Geschwindigkeit und schlechte Verbindungen.

Satelliten-Breitband

Eine drahtlose Hochgeschwindigkeits-Internetverbindung über Satellit. Manche Satelliten-Breitbandverbindungen sind bidirektional (aufwärts und abwärts). Andere Verbindungen gehen nur in eine Richtung: Der Satellit bietet eine Hochgeschwindigkeitsverbindung für den Downstream (vom Internet zum Benutzer) an, für den Upstream (vom Benutzer zum Internet) wird dagegen eine Einwahlverbindung oder ein anderes terrestrisches System verwendet.

Server

Ein Computer, der seine Ressourcen für andere Computer und Geräte im Netzwerk verfügbar macht. Dazu gehören z. B. Printserver, Internet-Server und Datenserver. Ein Server kann auch mit einem Switch oder Router kombiniert werden.

SSID (auch ESSID)

Eine eindeutige Kennzeichnung aus 32 Zeichen, die an den Header von über das WLAN versendeten Datenpaketen angehängt und als Passwort eingesetzt wird, wenn ein mobiles Gerät versucht, eine Verbindung zum BSS aufzubauen (siehe ESSID). Die SSID dient dazu, ein WLAN von anderen zu unterscheiden. Deshalb müssen alle Access Points und sonstigen Geräte, die versuchen, eine Verbindung zu einem bestimmten WLAN aufzubauen (siehe ESSID). Die SSID verwenden.

Geräten, die nicht über die eindeutige SSID verfügen, wird der Anschluss an das BSS verweigert. Da SSIDs jedoch den Paketen im Klartext zu entnehmen sind, bieten sie keinerlei Sicherheit für das Netzwerk. Die SSID wird auch als „Netzwerkname“ bezeichnet, da sie im Prinzip zur Kennzeichnung drahtloser Netzwerke dient.

SSL (Secure Sockets Layer)

Ein verbreitetes Verschlüsselungsprotokoll, das von vielen Online-Händlern und Online-Banking-Websites eingesetzt wird, um bei finanziellen Transaktionen Datensicherheit zu gewährleisten. Zu Beginn einer SSL-Sitzung sendet der Server seinen öffentlichen Schlüssel an den Browser. Der Browser sendet sodann einen nach dem Zufallsprinzip erstellten, geheimen Schlüssel zurück an den Server. Damit ist ein geheimer Schlüsselaustausch für diese Sitzung gewährleistet.

Standortprüfung

Untersuchung eines Standorts vor der Installation eines drahtlosen Netzwerks. Bei einer Standortprüfung wird der Standort auf seine Funk- und Benutzereigenschaften hin untersucht, um eine optimale Positionierung der Access Points zu erreichen.

Subnetz

Diese kleineren Netzwerke werden in großen Netzwerken eingesetzt, um die Adressierung zwischen zahlreichen Computern zu erleichtern. Subnetze werden über einen Router, Switch oder ein Gateway mit dem zentralen Netzwerk verbunden. Ein WLAN verwendet in der Regel für alle lokalen Computer, mit denen es kommuniziert, dasselbe Subnetz.

Switch

Ein Hub-ähnlicher Netzwerkverteiler, der die Nutzung eines Netzwerkes durch unterschiedliche Geräte effizient steuert, damit alle Geräte optimale Leistung erbringen können. Switches übernehmen im Netzwerk die Rolle eines Datenverkehrspolizisten: Während ein Hub alle empfangenen Pakete an sämtliche Ports weiterleitet, sendet ein Switch die Pakete nur an den Port, für den sie bestimmt sind.

TCP (Transmission Control Protocol)

Ein Protokoll, das zusammen mit dem Internet Protocol (IP) verwendet wird, um Daten in Form von einzelnen Einheiten, den sog. Paketen, über das Internet zwischen Computern zu versenden. IP ist dabei für die Zustellung der Daten zuständig, TCP protokolliert die einzelnen Pakete, in die eine Nachricht für das effiziente Routing über das Internet zerlegt wird.

Wenn beispielsweise eine Webseite von einem Webserver heruntergeladen wird, teilt die TCP-Programmschicht auf diesem Server die Datei in Pakete, versieht sie mit einer Nummer und leitet sie dann einzeln an die IP-Programmschicht weiter. Auch wenn alle Pakete dieselbe IP-Adresse als Ziel haben, können die einzelnen Pakete auf unterschiedlichen Wegen dorthin gelangen. Am anderen Ende fügt TCP die einzelnen Pakete wieder zusammen und wartet, bis alle angekommen sind, um sie dann als eine einzige Datei weiterzuleiten.

TCP/IP

TCP/IP ist das zugrunde liegende Protokoll, das die Kommunikation zwischen Computern im Internet und in einem Netzwerk ermöglicht. Der erste Teil, TCP, ist für die Übermittlung der Daten zuständig. TCP passt die Größe der Nachrichten an beiden Enden der Übertragung an und stellt sicher, dass die Nachricht richtig zugestellt wird. Der zweite Teil, IP, ist die Computeradresse eines Benutzers in einem Netzwerk. Jeder Computer in einem TCP/IP-Netzwerk hat eine eigene IP-Adresse, die ihm entweder dynamisch beim Systemstart oder aber permanent zugewiesen wird. Alle TCP/IP-Nachrichten enthalten die Adresse des Zielnetzwerks sowie die Adresse der Zielstation. So können TCP/IP-Nachrichten an mehrere Netzwerke (Subnetze) innerhalb eines Unternehmens oder in der ganzen Welt übermittelt werden.

TKIP (Temporal Key Integrity Protocol)

Eine Sicherheitsfunktion zur Verbesserung von WEP: TKIP und MIC (Message Integrity Check) sind Modifikationen von WEP zum Schutz gegen bekannte Angriffe (WEP und vier Patches für paketweises Ändern von Schlüsseln, Nachrichtenintegrität, Neuverschlüsselung und Initialisierungsvektorschutz).

Unternehmensnetzwerke: Benutzerauthentifizierung über 802.1x/EAP und RADIUS

WEP verfügt über nahezu keine Mechanismen zur Benutzerauthentifizierung. Zur Stärkung der Benutzerauthentifizierung implementiert WPA (Wi-Fi Protected Access) 802.1x und EAP (Extensible Authentication Protocol). Zusammengenommen bilden diese Verbesserungen das Gerüst für eine leistungsfähige Benutzerauthentifizierung. Dieses Gerüst verwendet einen zentralen Authentifzierungsserver, z. B. einen RADIUS-Server, um jeden Benutzer vor der Anmeldung beim Netzwerk zu authentifizieren. Eine gegenseitige Authentifizierung verhindert zudem, dass der Benutzer sich versehentlich bei einem Spionagenetzwerk anmeldet, das seine Anmeldedaten stiehlt.

USB (Universal Serial Bus)

Eine bidirektionale, serielle Hochgeschwindigkeitsverbindung zwischen einem PC und einem Peripheriegerät, die Daten bei 12 MBit/s überträgt. Der neue Standard USB 2.0 bietet sogar eine Übertragungsrate von bis zu 480 MBit/s. IEEE 1394, FireWire und iLink bieten allesamt eine Bandbreite von bis zu 400 MBit/s.

Verbesserte Datenverschlüsselung mit TKIP

Zur Verbesserung der Datenverschlüsselung setzt WPA (Wi-Fi Protected Access) TKIP (Temporal Key Integrity Protocol) ein. TKIP bietet wichtige Verbesserungen zur Datenverschlüsselung, darunter eine Funktion zum paketweisen Ändern von Schlüsseln, die Nachrichtenintegritätsprüfung Michael (Message Integrity Check, MIC), einen erweiterten Initialisierungsvektor (IV) mit Sequenzierungsregeln und einen Mechanismus zur Neuverschlüsselung. Mit diesen Verbesserungen berücksichtigt TKIP alle bekannten Schwächen von WEP.

Verschlüsselungscode

Eine alphanumerische (aus Buchstaben und Ziffern bestehende) Zeichenfolge, die die Verschlüsselung und Entschlüsselung von Daten für einen sicheren Datenaustausch unter den Mitgliedern eines Netzwerks ermöglicht. WEP verwendet einen Verschlüsselungscode, der ausgehende Daten im drahtlosen Netzwerk automatisch verschlüsselt. Auf der Empfängerseite kann der Computer die Informationen mit Hilfe desselben Verschlüsselungscodes automatisch entschlüsseln.

Voice over IP (VoIP, auch als IP-Telefonie bekannt)

Sprachübertragung, bei der mit Hilfe von IP digitale Pakete zum Versand über das Internet erstellt werden. VoIP kann kostengünstiger sein als die Sprachübertragung in herkömmlichen analogen Paketen über POTS (Plain Old Telephone Service, ein international gebräuchliches Synonym für den analogen Telefondienst).

VPN (Virtual Private Network)

Ein Verfahren, das die Sicherheit bei der Datenübertragung über das Internet erhöhen soll. VPN kann bei kabelgebundenen und drahtlosen Netzwerken sowie bei Einwahlverbindungen über analoge Telefonleitungen eingesetzt werden. VPN richtet einen privaten, verschlüsselten Tunnel ein, der vom Computer des Endbenutzers durch das drahtlose Netzwerk und das Internet hindurch bis hin zu den Unternehmensservern und -datenbanken reicht.

Warchalking

Das Anbringen von Kreidemarkierungen an Mauern, Gehwegen, Gebäuden, Schildern, Bäumen usw., um das Bestehen eines offenen drahtlosen Netzwerks, in der Regel mit einer Internetverbindung, zu kennzeichnen. So können Eingeweihte erkennen, wo sie gratis eine drahtlose Verbindung nutzen können. Die offenen Verbindungen stammen meist von den Access Points von drahtlosen Unternehmensnetzwerken in den Gebäuden. Die Kreidesymbole lassen erkennen, welche Art von Access Point an dieser spezifischen Stelle verfügbar ist.

Derzeit werden drei Hauptzeichen verwendet: Zwei Rücken an Rücken positionierte Halbkreise verweisen auf einen offenen Knoten, ein geschlossener Kreis zeigt einen geschlossenen Knoten an und ein geschlossener Kreis mit einem „W“ in der Mitte steht für einen Knoten, bei dem WEP aktiviert ist. Warchalker geben zudem über den Symbolen oft das Passwort an, das zum Zugreifen auf den Knoten erforderlich ist. Dies kann mit Hilfe von Sniffer-Software leicht ermittelt werden.

Da Warchalking relativ neu ist, ist die Debatte über dessen Legalität noch nicht abgeschlossen.

Es geht zurück auf wandernde Arbeiter in den USA der dreißiger Jahre, die ähnliche Markierungen an Häusern hinterließen, um anderen Wanderern zu signalisieren, ob dieses Haus Reisenden gegenüber aufgeschlossen war oder nicht.

Wardriving

Wardriving ist das Aufspüren und unter Umständen auch Nutzen von Verbindungen zu WLANs in Städten oder anderen Umgebungen. Zum Wardriving benötigt man ein Fahrzeug, einen Computer (z. B. ein Notebook), eine drahtlose Netzwerkkarte im Mixmode und eine Antenne, die auf dem Dach oder im Inneren des Autos angebracht werden kann. Da die Reichweite eines drahtlosen LAN oft über das jeweilige Bürogebäude hinausgeht, können sich Eindringlinge von außen Zugang zum Netzwerk verschaffen, eine kostenlose Internetverbindung nutzen und vielleicht sogar auf Unternehmensunterlagen und andere Ressourcen zugreifen.

Manche Leute betreiben Wardriving als eine Art Sport, teilweise auch um aufzuzeigen, wie anfällig WLANs für derartige Angriffe sind. Mit Hilfe einer omnidirektionalen Antenne und eines Positionierungssystems (GPS) kann der Wardriver die Standorte der 802.11b-Wireless-Access-Points systematisch bestimmen.

WEP (Wired Equivalent Privacy)

Das durch WiFi bereitgestellte grundlegende Verschlüsselungsverfahren für drahtlose Netzwerke. In manchen Fällen reicht WEP vollkommen aus, um die Sicherheitsanforderungen von Heimanwendern und kleinen Unternehmen im drahtlosen Netzwerk zu erfüllen. Bei WEP sind Verschlüsselungsmodi mit 40 Bit (oft auch als 64-Bit-Verschlüsselung bezeichnet) oder 104 Bit (oft auch als 128-Bit-Verschlüsselung bezeichnet) verfügbar. Da bei der 104-Bit-Verschlüsselung ein längerer Algorithmus verwendet wird, der aufwendiger zu entschlüsseln ist, kann sie größeren Schutz bieten als die einfache 40-Bit-(64-Bit-)Verschlüsselung.

WiFi (Wireless Fidelity)

Eine andere Bezeichnung für den Standard IEEE 802.11b. Produkte mit WiFi-Zertifizierung sind vollständig miteinander kompatibel, selbst wenn sie von unterschiedlichen Herstellern stammen. Ein Benutzer eines WiFi-Produkts kann einen Access Point einer beliebigen Marke mit Client-Hardware jeder anderen Marke kombinieren, solange beide Geräte dem WiFi-Standard entsprechen.

Wi-Fi Alliance (früher WECA, Wireless Ethernet Compatibility Alliance)

Die Wi-Fi Alliance ist eine gemeinnützige internationale Vereinigung, die 1999 gegründet wurde, um die Kompatibilität von WLAN-Produkten des Standards IEEE 802.11 zu zertifizieren. Derzeit sind 193 Unternehmen aus aller Welt Mitglied der Wi-Fi Alliance und 509 Produkte haben seit Beginn der Zertifizierung im März 2000 die WiFi-Zertifizierung erhalten. Die Zielsetzung der Wi-Fi Alliance und ihrer Mitglieder ist eine Verbesserung der Benutzerfreundlichkeit durch Produktkompatibilität (*www.weca.net*).

WiMAX

Eine IEEE 802.16-Arbeitsgruppe, die einen Standard für feste drahtlose Breitbandzugangssysteme auf Grundlage einer PMP-Architektur (Point-to-Multipoint) festlegt. Arbeitsgruppe 1 des Bereichs IEEE 802.16 hat einen Standard für den drahtlosen PMP-Breitbandzugang für Systeme im Frequenzbereich 10–66 GHz entwickelt. Der Standard gilt sowohl für die MAC- (Media Access Control) als auch für die Bitübertragungsschicht.

Wireless Multimedia (WMM)

WMM (Wireless Multimedia) ist eine Untergruppe des Standards 802.11e. Mit WMM kann drahtlos versendeten Daten je nach Datentyp eine unterschiedliche Priorität gegeben werden. Daten, bei denen Zeit eine wichtigere Rolle spielt (z. B. Video-, Audio- oder Sprachdaten) erhalten eine höhere Priorität als zeitlich unkritische Daten. WMM funktioniert jedoch nur, wenn die drahtlosen Clients WMM-fähig sind.

WLAN (Wireless LAN)

Wird manchmal auch als „LAN“ bezeichnet. Ein LAN, das für die Kommunikation zwischen den einzelnen Knoten Hochfrequenzfunkwellen statt Kabeln verwendet.

WPA (Wi-Fi Protected Access)

WPA ist ein Verschlüsselungsverfahren für drahtlose Netzwerke, das die Authentifizierung und Verschlüsselung gegenüber WEP (Wired Equivalent Privacy) verbessert. WPA wurde von der Netzwerkbranche als Reaktion auf die Schwächen von WEP entwickelt.

Ein wichtiger Teil von WPA ist das Protokoll TKIP (Temporal Key Integrity Protocol). TKIP behebt die Verschlüsselungsschwächen von WEP. Eine weitere zentrale Komponente von WPA ist die integrierte Authentifizierung (die in WEP nicht enthalten ist). Dank dieser Funktion kann WPA ein Sicherheitsniveau erreichen, das sich in etwa mit dem eines VPN-Tunnels mit WEP vergleichen lässt, wobei WPA sich jedoch deutlich einfacher verwalten und benutzen lässt. WPA funktioniert ähnlich wie 802.1x-Unterstützung und erfordert einen RADIUS-Server für die Implementierung. Die Wi-Fi Alliance wird diese Form von WPA als „WPA-Enterprise“ bezeichnen.

Zu WPA gibt es auch eine Variante namens „WPA Pre-Shared Key“ (WPA-PSK). Diese bietet eine Authentifizierungsalternative zu einem teuren RADIUS-Server. WPA-PSK ist eine vereinfachte, aber immer noch sehr leistungsstarke Form von WPA, die besonders für drahtlose Heimnetzwerke geeignet ist. Zur Verwendung von WPA-PSK wird wie bei WEP ein statischer Schlüssel (auch als „Passphrase“ bezeichnet) festgelegt. Doch mit Hilfe von TKIP kann WPA-PSK diesen Schlüssel automatisch in bestimmten voreingestellten Zeitabständen ändern. So wird es sehr viel schwerer für Hacker, den Schlüssel zu finden und zu missbrauchen. Die Wi-Fi Alliance wird diese Form von WPA als „WPA-Personal“ bezeichnen.

WPA für Klein- und Heimbüros

In einem Heimnetzwerk oder einer SOHO-Umgebung (Small Office/Home Office), wo es keine zentralen Authentifizierungsserver und keinen EAP-Rahmen gibt, wird WPA in einem speziellen Modus ausgeführt. Dieser Modus, der oft auch als „Pre-Shared Key“ (PSK) bezeichnet wird, ermöglicht die Benutzung von manuell eingegebenen Schlüsseln oder Passwörtern und wurde für die bequeme Einrichtung durch Privatbenutzer entwickelt. Der Privatbenutzer muss lediglich beim Access Point oder drahtlosen Heim-Gateway sowie auf jedem PC, der zum WiFi-Netzwerk gehört, ein Passwort (das auch als „Hauptschlüssel“ oder „Master Key“ bezeichnet wird) eingeben. Alles weitere wird automatisch durch WPA geregelt. Erstens wird nur Geräten mit dem richtigen Passwort der Zugang zum Netzwerk gestattet, so dass Lauscher und andere nicht autorisierte Personen ausgesperrt werden. Zweitens startet das Passwort automatisch die TKIP-Verschlüsselung (siehe weiter oben).

WPA für Public Access

Die in WPA festgelegten Verschlüsselungs- und Authentifizierungsmechanismen sind auch für Anbieter von drahtlosen Internetdiensten (Wireless Internet Service Provider, WISP) interessant, die so genannte „Hot-Spots“ – öffentlich zugängliche WiFi-Access-Points – betreiben. Da sich die Benutzer meist nicht gegenseitig kennen, sind sichere Datenübertragung und Authentifizierung dort von besonderer Bedeutung. Die in WPA definierte Authentifizierungsfunktion aktiviert einen sicheren Zugriffssteuerungsmechanismus für die Dienstanbieter und für mobile Benutzer, die keine VPN-Verbindungen verwenden.

WPA für Unternehmen

WPA erfüllt die WLAN-Sicherheitsanforderungen von Unternehmen auf effektive Weise und bietet eine leistungsstarke Verschlüsselungs- und Authentifizierungslösung bis zur Ratifizierung des Standards IEEE 802.11i. In einem Unternehmen mit einer eigenen EDV-Abteilung sollte WPA in Verbindung mit einem Authentifizierungsserver (z. B. RADIUS) eingesetzt werden, um eine zentrale Steuerung und Verwaltung des Netzwerkzugangs zu ermöglichen. Bei einer solchen Implementierung kann auf zusätzliche Lösungen wie VPNs verzichtet werden, vor allem, wenn es nur darum geht, die drahtlose Verbindung mit dem Netzwerk sicherer zu gestalten.

WPA im „gemischten Modus“

In einem großen Netzwerk werden höchstwahrscheinlich die Access Points vor den WiFi-Clients ersetzt. Access Points können daher manchmal auch in einem „gemischten Modus“ betrieben werden, der sowohl WPA-Clients als auch die herkömmlichen WEP-Clients unterstützt. So nützlich dies für die Übergangszeit auch ist, hat die Unterstützung beider Arten von Client-Geräten doch sehr nachteilige Auswirkungen auf die Sicherheit, die so bei allen Geräten auf dem weniger sicheren WEP-Niveau liegt. Es lohnt sich daher für Unternehmen, den Wechsel zu WPA für alle WiFi-Clients und Access Points zu beschleunigen.

WPA und IEEE 802.11i im Vergleich

WPA wird mit dem derzeit vom IEEE entwickelten Sicherheitsstandard IEEE 802.11i kompatibel sein. WPA ist eine Untergruppe des aktuellen 802.11i-Entwurfs, die einige der bereits einsatzreifen Elemente des 802.11i-Entwurfs umsetzt, darunter 802.1x und TKIP. Diese Funktionen können zudem bei den meisten vorhandenen Produkten mit Wi-Fi-Zertifizierung mit Hilfe eines Software-Upgrades aktiviert werden. Die wichtigsten Elemente des 802.11i-Entwurfs, die nicht in WPA enthalten sind, sind sicheres IBSS, Secure Fast Handoff, sichere Deauthentifizierung und Abmeldung sowie verbesserte Verschlüsselungsprotokolle wie AES-CCMP. Diese Funktionen sind entweder noch in der Entwicklung oder es sind Hardware-Upgrades für ihre Implementierung erforderlich.